

(12)特許協力条約に基づいて公開された国際出願

(19)世界知的所有権機関  
国際事務局



(43)国際公開日  
2004年7月8日 (08.07.2004)

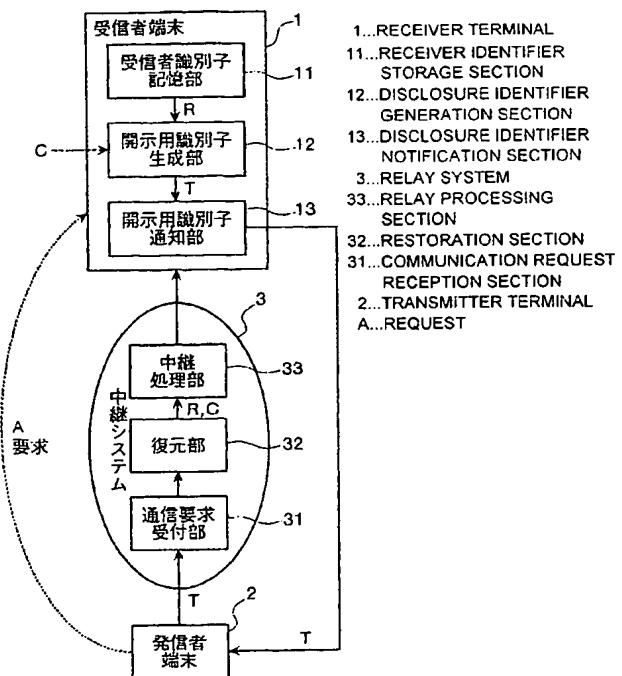
PCT

(10)国際公開番号  
WO 2004/057480 A1

(51)国際特許分類:	G06F 13/00, H04M 3/42, 3/50, H04L 9/00	特願 2003-352130 2003年10月10日 (10.10.2003) JP
(21)国際出願番号:	PCT/JP2003/016396	特願 2003-352131 2003年10月10日 (10.10.2003) JP
(22)国際出願日:	2003年12月19日 (19.12.2003)	(71)出願人(米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒100-8116 東京都千代田区 大手町二丁目3番1号 Tokyo (JP).
(25)国際出願の言語:	日本語	(72)発明者; および
(26)国際公開の言語:	日本語	(75)発明者/出願人(米国についてのみ): 川島 正久 (KAWASHIMA,Masahisa) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町3丁目9-11 NTT知的財産センター内 Tokyo (JP). 星野 文文学 (HOSHINO,Fumitaka) [JP/JP]; 〒180-8585 東京都 武蔵野市 緑町3丁目
(30)優先権データ:	特願 2002-369799 2002年12月20日 (20.12.2002) JP 特願2003-25976 2003年2月3日 (03.02.2003) JP	(76) /統葉有/

(54) Title: COMMUNICATION METHOD, COMMUNICATION SYSTEM, RELAY SYSTEM, COMMUNICATION PROGRAM, PROGRAM FOR COMMUNICATION SYSTEM, MAIL DISTRIBUTION SYSTEM, MAIL DISTRIBUTION METHOD, AND MAIL DISTRIBUTION PROGRAM

(54)発明の名称: 通信方法、通信システム、中継システム、通信プログラム、中継システム用プログラム、メール配送システム、メール配送方法およびメール配送プログラム



WO 2004/057480 A1

条件情報

(57) Abstract: A disclosure identifier generation section (12) of a receiver terminal (1) encrypts a receiver identifier R and communication condition information C stored in a receiver identifier storage section (11) and generates a disclosure identifier T. A disclosure identifier notification section (13) notifies this to a transmitter terminal (2). When a communication request using the disclosure identifier T is made from the transmitter terminal (2), a restoration section (32) of a relay system (3) extracts the communication condition information C from the disclosure identifier T and communication between the receiver terminal (1) and the transmitter terminal (2) is established only if the communication condition information is satisfied.

(57) 要約: 受信者端末 (1) の開示用識別子生成部 (12) により受信者識別子記憶部 (11) に記憶した受信者識別子 R と通信条件情報 C とを暗号化して開示用識別子 T を生成してこれを開示用識別子通知部 (13) が発信者端末 (2) に通知し、発信者端末 (11) から開示用識別子 T を用いた通信要求がなされた際に、中継システム (3) の復元部 (32) が開示用識別子 T から通信条件情報 C を抽出し、この通信

/統葉有/



9-11 NTT知的財産センタ内 Tokyo (JP). 藤村明子 (FUJIMURA,Akiko) [JP/JP]; 〒180-8585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 木下真吾 (KINOSHITA,Shingo) [JP/JP]; 〒180-8585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 中尾昌善 (NAKAO,Masayoshi) [JP/JP]; 〒180-8585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 斎藤典明 (SAITOU,Akinori) [JP/JP]; 〒180-8585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 鶴岡行雄 (TSURUOKA,Yukio) [JP/JP]; 〒180-8585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 高橋克巳 (TAKAHASHI,Katsuaki) [JP/JP]; 〒180-8585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 安部剛 (ABE,Tsuyoshi) [JP/JP]; 〒180-8585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP). 三宅潤 (MIYAKE,Jun) [JP/JP]; 〒180-8585 東京都武蔵野市緑町3丁目9-11 NTT知的財産センタ内 Tokyo (JP).

(74) 代理人: 酒井宏明, 外 (SAKAI,Hiroaki et al.); 〒100-0013 東京都千代田区霞が関三丁目2番6号 東京俱楽部ビルディング Tokyo (JP).

(81) 指定国(国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国(広域): ARIPO特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ヨーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 國際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイドノート」を参照。

Rec'd 11 JUN 2005

## 明 細 書

通信方法、通信システム、中継システム、通信プログラム、中継システム用プログラム、メール配送システム、メール配送方法およびメール配送プログラム

5

## 技術分野

この発明は、本発明は、受信者を一意に特定する受信者識別子を用いた発信者通信端末からの通信要求に応答して該発信者通信端末と受信者通信端末との通信をおこなう通信方法、通信システム、中継システム、通信プログラム、中継システム用プログラム、メール配送システム、メール配送方法およびメール配送プログラムに関するものである。

## 背景技術

従来より、電気通信事業者が運営する公衆電話網やインターネットサービスプロバイダが運営するサーバ等の中継システムでは、受信者を一意に識別可能な受信者識別子に応じて、当該受信者の通信端末（受信者通信端末）と任意の発信者の通信端末（発信者通信端末）との通信を確立していた。

すなわち、中継システムに対して任意の発信者が発信者通信端末において電話番号やメールアドレス等の受信者を一意に識別可能な受信者識別子を指定すると、中継システムはこの受信者識別子に基づいて受信者を特定し、特定した発信者の発信者通信端末と受信者通信端末との通信を確立（なお、ここでいう「通信の確立」とは、通信端末間にリアルタイムの通信路を設定する、一方の通信端末からのメールやデータを他方の通信端末へ送信する等のあらゆる意味を含むものとする）していた。

前述した受信者識別子は、通常、中継システムより基本的に1回線あるいは1受信者に付き1つ与えられ、受信者は事前にこの受信者識別子を、親戚、知人、取引先等の発信を希望する相手（発信者）に直接伝えたり、電話、FAX、手紙

、電子メール等の様々な手段で通知していた（特許文献1参照）。

特許文献1

特開平10-198613号公報

ところで、前述した受信者識別子は、受信者が懸賞に応募したり、通信販売を  
5 申し込んだりする際等に連絡先として通知することができ、このような受信者自身の行為によって発信を希望しない第三者に知られてしまうことがある。

受信者識別子が一旦、このような第三者に知られてしまうと、セールスや勧誘  
を目的とした迷惑電話や迷惑メールが頻繁に来るようになり、受信者の想定外の  
用途に利用されることが多くなって、事実上、その回線やメールアドレスが使用  
10 不可能になってしまった。

このような場合、受信者は、この受信者識別子を放棄し、中継システムから新た  
たな受信者識別子を取得していたが、新たな受信者識別子への連絡先の変更を複  
数の発信を希望する発信者に伝えなければならず、大きな手間がかかるという問  
題があった。

15 本発明は、このような従来の問題（課題）を解決し、受信者識別子が当該受信  
者の想定外の用途に利用されることを防ぐことができる通信方法、通信システム  
、中継システム、通信プログラム、中継システム用プログラム、メール配達シス  
テム、メール配達方法およびメール配達プログラムを提供することを目的とする  
。

20

発明の開示

本発明にかかる通信方法は、受信者に通信する際の通信条件を示す通信条件情  
報および受信者識別子に基づいて開示用識別子を生成しておき、生成した開示用  
25 識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識  
別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含  
まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者  
通信端末の通信を確立することを特徴とする。

また、本発明にかかる通信方法は、受信者通信端末に配送するメールの配送条件を示す配送条件情報および受信者を一意に特定する受信者アドレスに基づいて開示用アドレスを生成しておき、生成した開示用アドレスを宛先アドレスとするメールを受け付けた場合に、該メールの宛先アドレスである開示用アドレスから受信者アドレスおよび配送条件情報を復元し、復元した配送条件情報に包摂される配送条件を満たす場合に、メールを受信者通信端末に対して配送することを特徴とする。  
5

また、本発明にかかる通信方法は、受信者電話端末に通話接続する際の通話条件情報および受信者電話番号に基づいて開示用電話番号を生成しておき、生成した開示用電話番号に基づく通話接続要求を受け付けた場合に、該通話接続要求に含まれる開示用電話番号から受信者電話番号および通話条件情報を復元し、復元した通話条件情報に含まれる通話条件を満たす場合に、発信者電話端末と受信者電話端末とを通話接続することを特徴とする。  
10

また、本発明にかかる通信方法は、受信者通信端末において通信条件情報および受信者識別子に基づいて開示用識別子を生成することを特徴とする。  
15

また、本発明にかかる通信方法は、受信者通信端末と通信可能な所定の仲介装置において通信条件情報および受信者識別子に基づいて開示用識別子を生成することを特徴とする。

また、本発明にかかる通信方法は、受信者通信端末と送信者通信端末の間に介在する中継システムが、復元された受信者識別子および／または通信条件情報を受信者通信端末に通知することを特徴とする。  
20

また、本発明にかかる通信方法は、受信者通信端末と送信者通信端末の間に介在する中継システムが、復元された通信条件情報に含まれる通信条件を満たさない場合の処理内容を決定することを特徴とする。

また、本発明にかかる通信方法は、受信者通信端末が、復元された通信条件情報に含まれる通信条件を満たさない場合の処理内容を決定することを特徴とする  
25

また、本発明にかかる通信方法は、通信条件情報が、開示用識別子を開示する発信者を限定する発信者限定情報を含み、少なくとも通信要求をおこなった発信者が前記発信者限定情報に含まれる限定条件と一致すると判断した場合に、この通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立することを特徴とする。

また、本発明にかかる通信方法は、通信条件情報に開示用識別子を開示する開示先を特定する開示先特定情報を含ませることを特徴とする。

また、本発明にかかる通信方法は、復元された通信条件情報に含まれる通信条件を満たさない場合に、通信要求を拒絶することを特徴とする。

また、本発明にかかる通信方法は、復元した通信条件情報に含まれる通信条件を満たさない場合に、通信要求にかかわらず受信者通信端末と異なる所定の通信端末と発信者通信端末との通信を確立することを特徴とする。

また、本発明にかかる通信方法は、各受信者の受信者識別子および該受信者の受信者通信端末に通信する際の通信条件を示す通信条件情報を仲介装置に登録しておき、発信者通信端末から開示用識別子の開示要求を受け付けた場合に、この仲介装置に登録された受信者識別子および通信条件情報に基づいて開示用識別子を生成することを特徴とする。

また、本発明にかかる通信方法は、開示用識別子の開示要求をおこなう発信者が開示要求をおこなう資格を有するか否かを判定し、発信者が資格を有さないと判定された場合に通信要求を棄却することを特徴とする。

また、本発明にかかる通信方法は、受信者通信端末に通信する際の仮の通信条件を示す仮通信条件情報および受信者識別子に基づいて仮開示用識別子を生成し、生成した仮開示用識別子を仲介装置に登録しておき、発信者通信端末から開示用識別子の開示要求を受け付けた場合に、この仲介装置に登録された仮開示用識別子および通信条件情報を開示用識別子書換装置に送信して開示用識別子の書き換えを要求し、この要求に応答して仮開示用識別子および通信条件情報から開示用識別子を生成することを特徴とする。

また、本発明にかかる通信方法は、仲介装置が書換要求をおこなう資格を有するか否かを仮開示用識別子に基づいて判定し、当該仲介装置が資格を有さないと判定された場合に書換要求を棄却することを特徴とする。

また、本発明にかかる通信方法は、受信者識別子および通信条件情報を所定の公開鍵で暗号化して開示用識別子を生成し、生成した開示用識別子に基づく通信を受け付けた場合に、該開示用識別子を公開鍵に対応する秘密鍵で復号化して受信者識別子および通信条件情報を復元することを特徴とする。  
5

また、本発明にかかる通信方法は、所定の共通する鍵を用いて受信者識別子および通信条件情報を暗号化して開示用識別子を生成し、生成した開示用識別子に基づく通信を受け付けた場合に、該開示用識別子を当該共通する鍵で復号化して受信者識別子および通信条件情報を復元することを特徴とする。  
10

また、本発明にかかる通信方法は、受信者識別子および通信条件情報を所定の共通鍵で暗号化して開示用識別子を生成し、生成した開示用識別子に基づく通信を受け付けた場合に、該開示用識別子を共通鍵で復号化して受信者識別子および通信条件情報を復元することを特徴とする。  
15

また、本発明にかかる通信方法は、通信条件情報および受信者識別子に基づいて開示用識別子を生成する際に、通信条件情報を第三者による改竄ができない形式で開示用識別子に含めることを特徴とする。

また、本発明にかかる通信方法は、通信条件情報が通信条件の種別または組み合わせを含み、復元に際してはこの開示用識別子から通信条件の種別または組み合わせを抽出し、抽出した通信条件の種別および組み合わせにしたがって該開示用識別子から受信者識別子および通信条件情報を復元することを特徴とする。  
20

また、本発明にかかる通信システムは、開示用識別子付与装置が、受信者通信端末に通信する際の通信条件を示す通信条件情報を受信者識別子に基づいて開示用識別子を生成するとともに、生成した開示用識別子を発信者通信端末に通知し、中継システムは、開示用識別子付与装置により付与された開示用識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から  
25

受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立することを特徴とする。

また、本発明にかかる通信システムは、開示用識別子付与装置が受信者通信端末の一部をなすことを特徴とする。  
5

また、本発明にかかる通信システムは、開示用識別子付与装置が受信者通信端末および中継システムのいずれとも異なる仲介装置とすることを特徴とする。

また、本発明にかかる中継システムは、受信者通信端末に通信する際の通信条件を示す通信条件情報および受信者識別子に基づいて生成された開示用識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立することを特徴とする。  
10

また、本発明にかかる通信プログラムは、受信者に通信する際の通信条件を示す通信条件情報および受信者識別子に基づいて開示用識別子を生成しておき、生成した開示用識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立することを特徴とする。  
15

また、本発明にかかる中継システム用プログラムは、受信者通信端末に通信する際の通信条件を示す通信条件情報および受信者識別子に基づいて生成された開示用識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立することを特徴とする。  
20

また、本発明にかかるメール配送システムは、開示用アドレス発行装置が、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスに基づい

て開示用アドレスを発行し、メール転送装置が、開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから着信者アドレスの復元および配達条件情報の抽出をおこない、該抽出した配達条件情報に含まれる配達条件を当該メールが満たす場合に、該メールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送することを特徴とする。

また、本発明にかかるメール配達システムは、開示用アドレス発行装置が、着信者に配達するメールの配達条件を示す配達条件情報と着信者アドレスを受け付け、受け付けた配達条件情報と着信者アドレスを暗号化して開示用アドレスを生成し、生成した開示用アドレスを着信者通信端末に返信し、メール転送装置は、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して着信者アドレスの復元および配達条件情報の抽出をおこない、該抽出した配達条件情報に含まれる配達条件を満たすメールを抽出し、抽出したメールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送することを特徴とする。

また、本発明にかかるメール配達システムは、暗号鍵テーブルに登録した所定の暗号鍵を用いて配達条件情報と着信者アドレスを暗号化して開示用アドレスを生成し、暗号鍵テーブルに登録された各暗号鍵に対応する復号鍵を登録した復号鍵テーブルから復号鍵を取り出し、取り出した復号鍵を用いて開示用アドレスを復号化して着信者アドレスの復元および配達条件情報の抽出をおこなうことを特徴とする。

また、本発明にかかるメール配達システムは、暗号鍵テーブルに登録した所定の暗号鍵を用いて暗号化する暗号化対象データのデータ長が所定長未満である場合に該所定長を満たすように乱数を付加することを特徴とする。

また、本発明にかかるメール配達システムは、複数の暗号鍵にそれぞれ鍵識別子を対応付けて暗号鍵テーブルに登録し、配達条件情報と着信者アドレスを暗号化する際に用いた暗号鍵の鍵識別子を開示用アドレスに含め、開示用アドレスから抽出した鍵識別子を有する復号鍵を復号鍵テーブルから取り出し、取り出した

復号鍵を用いて開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこなうことを特徴とする。

また、本発明にかかるメール配送システムは、暗号鍵テーブルと復号鍵テーブルは、複数の共通鍵にそれぞれ鍵識別子を対応付けて登録した同一のテーブルとすることを特徴とする。  
5

また、本発明にかかるメール配送システムは、複数の公開鍵をそれぞれ鍵識別子と対応付けて暗号鍵テーブルに登録し、この暗号鍵テーブルに登録された各公開鍵に対応する秘密鍵をそれぞれ同じ鍵識別子に対応づけて復号鍵テーブルに登録することを特徴とする。

10 また、本発明にかかるメール配送システムは、開示用アドレスへの通信の利用を許可する発信者アドレス、開示用アドレスへの通信の利用を許可する発ドメイン、開示用アドレスの有効期限または開示用アドレスの有効開始日若しくはこれらの組み合わせを配送条件情報とすることを特徴とする。

15 また、本発明にかかるメール配送システムは、指定された配送条件の種別・組み合わせを開示用アドレスに含めることを特徴とする。

また、本発明にかかるメール配送システムは、発信者アドレスまたは発ドメインを配送条件情報とする場合に、該発信者アドレスまたは発ドメインのハッシュ値の全部または一部を開示用アドレスに含めることを特徴とする。

20 また、本発明にかかるメール配送システムは、複数の乱数列を記憶する乱数列テーブルから抽出した乱数列を用いて暗号化対象となる情報の一部を可逆変換処理することを特徴とする。

また、本発明にかかるメール配送システムは、開示用アドレスの生成に用いられる情報の一部に基づき乱数列テーブルから抽出する乱数を決定することを特徴とする。

25 また、本発明にかかるメール配送システムは、配送条件情報に基づいて乱数列テーブルから乱数列を選択し、選択した乱数列を用いて着信者アドレスを可逆変換処理することを特徴とする。

また、本発明にかかるメール配送システムは、開示用アドレス発行装置およびメール転送装置に対して、各着信者アドレスを所定のアドレス識別子に対応付けて記憶するアドレステーブルを設け、着信者アドレスに対応するアドレステーブルに記憶したアドレス識別子と配送条件情報を暗号化して開示用アドレスを生成し、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化してアドレス識別子の復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、開示用アドレスから復元したアドレス識別子に対応する前記アドレステーブルに記憶した着信者アドレスにメールの宛先を置き換えて当該メールを転送することを特徴とする。

また、本発明にかかるメール配送方法は、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスに基づいて開示用アドレスを発行し、開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから着信者アドレスの復元および配送条件情報の抽出をおこない、抽出した配送条件情報に含まれる配送条件を当該メールが満たす場合に、該メールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送することを特徴とする。

また、本発明にかかるメール配送方法は、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスを受け付け、受け付けた配送条件情報と着信者アドレスを暗号化して開示用アドレスを生成し、生成した開示用アドレスを着信者通信端末に返信するとともに、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、抽出したメールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送することを特徴とする。

また、本発明にかかるメール配送方法は、暗号鍵テーブルに登録した所定の鍵識別子を有する暗号鍵を用いて受け付けた配送条件情報と着信者アドレスを暗号化して開示用アドレスを生成し、所定の鍵識別子を有する復号鍵を復号鍵テーブ

ルから取り出し、取り出した復号鍵を用いて開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこなうことを特徴とする。

また、本発明にかかるメール配送方法は、開示用アドレスの利用を許可する発信者アドレス、開示用アドレスの利用を許可する発ドメイン、開示用アドレスの有効期限または開示用アドレスの有効開始日若しくはこれらの組み合わせを配送条件情報とすることを特徴とする。  
5

また、本発明にかかるメール配送方法は、指定された配送条件の種別・組み合わせを開示用アドレスに含めることを特徴とする。

また、本発明にかかるメール配送方法は、各着信者アドレスを所定のアドレス識別子に対応付けてアドレステーブルに記憶しておき、着信者アドレスに対応するアドレステーブルに記憶したアドレス識別子と配送条件情報を暗号化して開示用アドレスを生成するとともに、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化してアドレス識別子の復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、開示用アドレスから復元したアドレス識別子に対応するアドレステーブルに記憶した着信者アドレスにメールの宛先を置き換えて当該メールを転送することを特徴とする。  
10  
15

また、本発明にかかるメール配送プログラムは、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスに基づいて開示用アドレスを発行するとともに、開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから着信者アドレスの復元および配送条件情報の抽出をおこない、抽出した配送条件情報に含まれる配送条件を当該メールが満たす場合に、該メールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送することを特徴とする。  
20  
25

また、本発明にかかるメール配送プログラムは、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスを受け付け、受け付けた配送条件情報と記着信者アドレスを暗号化して開示用アドレスを生成し、生成した開示用ア

5 ドレスを着信者通信端末に返信するとともに、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、抽出したメールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送することを特徴とする。

10 また、本発明にかかるメール配送プログラムは、暗号鍵テーブルに登録した所定の鍵識別子を有する暗号鍵を用いて配送条件情報と着信者アドレスを暗号化して開示用アドレスを生成するとともに、所定の鍵識別子を有する復号鍵を復号鍵テーブルから取り出し、取り出した復号鍵を用いて開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこなうことを特徴とする。

15 また、本発明にかかるメール配送プログラムは、開示用アドレスの利用を許可する発信者アドレス、開示用アドレスの利用を許可する発ドメイン、開示用アドレスの有効期限または前記開示用アドレスの有効開始日若しくはこれらの組み合わせを配送条件情報とすることを特徴とする。

20 また、本発明にかかるメール配送プログラムは、指定された配送条件の種別・組み合わせを開示用アドレスに含めることを特徴とする。

25 また、本発明にかかるメール配送プログラムは、各着信者アドレスを所定のアドレス識別子に対応付けてアドレステーブルに記憶しておき、着信者アドレスに対応するアドレステーブルに記憶したアドレス識別子と配送条件情報を暗号化して開示用アドレスを生成するとともに、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化してアドレス識別子の復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、開示用アドレスから復元したアドレス識別子に対応するアドレステーブルに記憶した着信者アドレスにメールの宛先を置き換えて当該メールを転送することを特徴とする。

第1図は、本実施例1に係る通信システムの構成を示す図であり、第2図は、第1図に示した実施例1の処理手順を示すシーケンス図であり、第3図は、本実施例1に係るメールシステムのシステム構成を示す機能ブロック図であり、第4図は、第3図に示した受信者端末の処理手順を示すフローチャートであり、第5図は、開示用アドレス生成ページの一例を示す図であり、第6図は、第3図に示した開示用アドレス生成部による開示用アドレスの生成要領を説明するための説明図であり、第7図は、第3図に示したフィルタリングサーバの処理手順を示すフローチャートであり、第8図は、第3図に示した通信条件情報抽出部およびメール転送処理部によるフィルタリングの実施要領を説明するための説明図であり、第9図は、本実施例2に係る通信システムの構成を示す図であり、第10図は、第9図に示した実施例2の処理手順を示すシーケンス図であり、第11図は、開示用アドレスの生成とフィルタリングの両方をおこなう開示用メール処理サーバを設けた場合のシステム構成を示す図であり、第12図は、本実施例3に係る通信システムの構成を示す図であり、第13図は、第12図に示した実施例3の処理手順を示すシーケンス図であり。第14図は、本実施例4に係る電話交換システムのシステム構成を示す機能ブロック図であり、第15図は、第14図に示した着信者用電話機、開示用電話番号処理装置および発信者用電話機の処理手順を示すシーケンス図であり、第16図は、第14図に示した電話番号通知処理部の処理手順を示すフローチャートであり、第17図は、第14図に示した開示用電話番号生成部による開示用電話番号の生成要領を説明するための説明図であり、第18図は、第14図に示したフィルタリング処理部の処理手順を示すフローチャートであり、第19図は、第14図に示した通話条件情報抽出部および回線接続指示部によるフィルタリングの実施要領を説明するための説明図であり、第20図は、インターネット上のWEBサーバを利用して開示用電話番号の通知を依頼する場合のシステム構成を示す図であり、第21図は、開示用電話番号生成ページの一例を示す図であり、第22図は、第3図に示したフィルタリングサーバのハードウェア構成を示すブロック図であり、第23図は、実施例1の受信者

端末を実現するプログラムの流れを示すフローチャートであり、第24図は、実施例1の中継システムを実現するプログラムの流れを示すフローチャートであり、第25図は、実施例2の仲介装置を実現するプログラムの流れを示すフローチャートであり、第26図は、実施例3の仲介装置を実現するプログラムの流れを示すフローチャートであり、第27図は、実施例3の開示用識別子書換装置を実現するプログラムの流れを示すフローチャートである。

また、第28図は、本実施例5に係るメール配達システムのシステム構成を示す図であり、第29図は、第28図に示した暗号鍵テーブルの一例を示す図であり、第30図は、第28図に示したユーザテーブルの一例を示す図であり、第31図は、第28図に示した条件コードテーブルの一例を示す図であり、第32図は、第28図に示したアドホックアドレス発行サーバによるアドホックアドレスの発行手順を示すシーケンス図であり、第33図は、ユーザ認証ページの一例を示す図であり、第34図は、アドホックアドレス発行ページの一例を示す図であり、第35図は、第32図のステップS170に示したアドホックアドレス生成処理手順を示すフローチャートであり、第36図は、アドホックアドレス生成の具体例を示す図であり、第37図は、第28図に示したアドホックメール転送サーバによるアドホックメールの転送手順を示すシーケンス図であり、第38図は、第37図のステップS304で示したフィルタ処理手順を示すフローチャートであり、第39図は、本実施例6に係るメール配達システムのシステム構成を示す図であり、第40図は、第39図に示した乱数列テーブルの一例を示す図であり、第41図は、第39図に示したアドホックアドレス生成部によるアドホックアドレス生成の具体例を示す図であり、第42図は、本実施例7に係るメール配達システムのシステム構成を示す図であり、第43図は、第42図に示したアドレステーブルの一例を示す図である。

#### 発明を実施するための最良の形態

以下に添付図面を参照して、この発明に係る通信方法、通信システム、中継シ

システム、通信プログラムおよび中継システム用プログラムの実施例を図面に基づいて詳細に説明する。なお、以下に示す実施例1～3では本発明をメールアドレスに適用した場合を示し、実施例4では本発明を電話番号に適用した場合を示すこととする。

5 (実施例1)

まず、本発明の概要と前提となる技術について述べる。

ところで、たとえ膨大な数の開示用識別子が付与されていたとしても、それが連続する整数であるような場合は、1つの開示用識別子を破棄しても悪意ある発信者なら容易に類推できる他の開示用識別子を用いて用途外利用をおこなう可能性がある。また、本発明では、通信条件情報を開示用識別子に埋め込むため、この通信条件情報を不正に改竄できないようにする必要がある。これらのことから10、本発明では暗号技術を利用する。

<公開鍵暗号>

15 公開鍵暗号は、暗号化するための鍵（暗号鍵）と復号するための鍵（復号鍵）とが異なる暗号方式である。公開鍵暗号で暗号文を受け取る者は、まず1対の暗号鍵と復号鍵を生成し、暗号鍵を公開し、復号鍵は秘密に保持する。暗号鍵は公開されているので、誰でも上記暗号文を受け取る者に対して暗号文を送ることができる。

<ハイブリッド暗号>

20 公開鍵暗号は一般に暗号化あるいは復号するのに大きな演算量を必要としており、長いメッセージの暗号化や復号化には向いていない。長いメッセージを暗号化するには、乱数（セッション鍵）を生成し、それを公開鍵暗号で暗号化し、メッセージはセッション鍵を用いて共通鍵暗号により暗号化することにより、長いメッセージでも効率良く暗号文を送ることができる。この公開鍵暗号及び共通鍵暗号の使用方法を一般にハイブリッド暗号と呼ぶ。本発明では、特に断らない限り、このハイブリッド暗号を含め公開鍵暗号と呼ぶ。

<改竄防止>

攻撃者による、上記のような不正な開示用識別子の生成による攻撃を防ぐことを目的として、改竄防止コードを平文または暗号文に付加することが可能である。メッセージ認証子（MAC）やデジタル署名を使えば上記のような改竄を防止することができる。また、共通鍵暗号あるいは上述した広義の公開鍵暗号には使用方法によって改竄防止機能を持つものがある。そのような暗号系を利用する場合には暗号系が持つ改竄防止機能を利用しても良い（例えば、岡本龍明、山本博 著「現代暗号」産業図書株式会社、ISBN 4-7828-5353-X、1997年6月30日発行、P163～187参照）。

＜公開鍵暗号系を使った方法＞

10 本発明では類推不能な膨大な数の開示用識別子の集合を作るために公開鍵暗号系を用いる。具体的には、下記通信を行う。

0：電気通信事業者等が運営する中継システムが公開鍵を用意し、これを公開する。

15 1：受信者の受信者識別子を記憶する記憶部を備えた装置が上記公開鍵を用いて、受信者識別子に所定の通信条件情報、例えば相手を特定する識別子、あるいは受信（または中継）を許可するか拒絶するかを決定するためのデータ（受信条件）、あるいは乱数、あるいはそれらの組み合わせを付加して暗号化する。暗号化されたデータを開示用識別子として発信者の通信端末へ通知する。

20 2：発信者の通信端末が中継システムに対して上記開示用識別子を指定して発信する。

3：中継システムは上記開示用識別子を上記公開鍵に対応する秘密鍵を使って復号し、受信者識別子を取得して受信者を特定する。

次に、本実施例1にかかる通信システムの基本構成について説明する。第1図において、1は受信者の通信端末（受信者端末）、2は発信者の通信端末（発信者端末）、3は中継システムであり、受信者端末1は受信者識別子記憶部11と開示用識別子生成部12と開示用識別子通知部13とを備え、中継システム3は通信要求受付部31と復元部32と中継処理部33とを備えている。なお、この

開示用識別子生成部 1 2 の処理は請求項 1 の開示用識別子生成工程に対応し、復元部 3 2 の処理は請求項 1 の復元工程に対応し、中継処理部 3 3 の処理は請求項 1 の通信確立工程に対応する。また、受信者端末 1 が請求項 2 2 の開示用識別子付与装置に対応し、中継システム 3 が請求項 2 2 の中継システムに対応する。この場合に、開示用識別子生成部 1 2 、復元部 3 2 および中継処理部 3 3 がそれぞれ請求項 2 2 の開示用識別子生成手段、復元手段および通信確立手段に対応することになる。  
5

受信者端末 1 の開示用識別子生成部 1 2 は、受信者識別子記憶部 1 1 に記憶された受信者識別子 R と、別途記憶されもしくは入力された所定の通信条件情報 C とから、中継システム 3 の運用者以外も実行可能な方法で開示用識別子 T を生成し、開示用識別子通知部 1 3 により発信者端末 2 へ通知（開示）する。  
10

発信者端末 2 は、開示用識別子 T を指定して中継システム 3 に通信を要求する。中継システム 3 が、通信要求受付部 3 1 が開示用識別子 T を指定した通信要求を受信すると、復元部 3 2 は中継システム 3 の運用者のみが実行可能な方法で開示用識別子 T を復号して受信者識別子 R と通信条件情報 C を取得する。中継処理部 3 3 は、通信条件情報に含まれる通信条件を満たす場合には、受信者識別子 R 15 を着信先として通信要求を処理する。

開示用識別子 T は、受信者識別子 R と所定の通信条件情報 C とを連結してできる情報列を中継システム 3 の運用者の公開鍵で暗号化することにより生成できる。この場合、中継システム 3 は、公開鍵に対応する秘密鍵で開示用識別子を復号し、受信者識別子 R 及び通信条件情報 C を取得することになる。  
20

ここで、かかる通信条件情報 C に当該開示用識別子 T の開示先の識別子を含めれば、当該開示用識別子 T を宛先とした迷惑なメールや電話を受信した場合に、この開示用識別子 T が誰を経由して漏洩したかを認識できるため、受信者識別子の漏洩を抑止できる。  
25

また、この通信条件情報 C に発信者または発信者端末を限定する情報や利用可能期間を限定する情報を含ませることにより、開示用識別子 T の利用条件を限定

することができる

。発信者または発信者端末を限定する情報の例として、発信者または発信者端末の識別子やこの識別子から計算されるハッシュ値がある。また、利用可能期間を限定する情報の例として、開示用識別子Tの有効期限、有効時間帯（夜間禁止など）などがある。

この場合、中継システム3の中継処理部33として、取得した受信者識別子または所定の通信条件情報をもしくはその両方に基づき、通信要求を許可するか拒絶するかを決定することになる。

また、中継システム3は、取得した受信者識別子または受信者識別子及び所定の通信条件情報を含む通信要求をそのまま受信者端末1へ通知し、当該受信者端末1において受信者識別子または所定の通信条件情報をもしくはその両方に基づき、通信要求を許可するか拒絶するかを決定することもできる。なお、開示用識別子は発信者毎に異なるものを付与する必要があり、また、利用期限を限定した場合には期限が経過する度に再付与する必要がある。

次に、上記通信システムのシステム構成を前提とした実施例1の内容について詳細に説明する。なお、ここでは本発明を電子メールシステムに適用した場合を示すこととし、具体的にはあるインターネットサービスプロバイダ（ISP）がユーザ向けに本発明を用いた電子メール通信サービスをしていると想定する。受信者端末は当該ISPのユーザの端末とする。また、受信者識別子は当該ISPのユーザの電子メールアドレスであり、“ユーザ名@user.com”という形式のドメイン名を有する。

また、中継システムは、本発明に基づくアドレス処理機能を備えた電子メール中継サーバ3aと、受信者識別子を宛先とするメールを中継する標準的な電子メール中継サーバ3bとを含むものとする。

電子メール中継サーバ3aは、市販の汎用サーバ機に本発明に基づくアドレス処理を実行するプログラムを動作させることにより実現する。電子メール中継サーバ3aのホスト名はpcode.comとする。

なお、受信者端末はインターネット通信機能を備えるコンピュータに、本発明に基づく処理を実行するプログラム動作させることにより実現する。なお、発信者端末のユーザは当該 I S P のユーザでなくても良い。

第 2 図は、本発明に係る通信システムの処理手順を示すシーケンス図である。

5 まず、中継システム 3 は、秘密鍵と公開鍵のペアを用意するとともに、このうちの公開鍵について公開し (S t e p 1) 、受信者端末 1 は、中継システム 3 が公開する公開鍵を用いて受信者識別子及び所定の通信条件情報を暗号化して開示用識別子を生成する (S t e p 2) 。

10 具体的には、受信者端末 1 を使用する受信者の電子メールアドレスの @ よりも前の文字列 (ユーザ名部分) N と通信条件情報 C とを適当な連結子 ("+" など) で連結し、該連結した文字列を I S P の公開鍵を用いて暗号化する。そして、暗号化された暗号データをテキスト化して文字列とし、該文字列に対して "@ p c o d e . c o m" というドメイン名を追加したメールアドレスを開示用識別子 T として生成する。

15 ここで、上記通信条件情報 C は、種別を示す文字 c 1 と、種別依存制御情報 c 2 とによって形成され、通信を許可するか拒絶するかの条件 (受信条件) をかかる通信条件情報 C に含めることができる。たとえば発信者を限定する場合には、 c 1 を "S" 、 c 2 を発信者アドレスのハッシュ値とし、識別子の有効期限を限定する場合には、 c 1 を "T" 、 c 2 を有効期限とする。また、発信者アドレスのドメイン名を指定する場合には、 c 1 を "O" とし、 c 2 を当該指定ドメイン名のハッシュ値とする。また、発信者アドレスと有効期限を指定する場合には、 c 1 を "P" とし、 c 2 の最初の 6 文字を発信者アドレスのハッシュ値、 7 文字目以降を有効期限とする。

20 また、通信条件情報 C には、受信条件を定めない種別を定義することもでき、この場合に生成される開示用識別子は、受信条件付きではない開示用識別子となる。例えば、開示用識別子の開示を受けた者が、当該受信者の承諾を得ずに第 3 者に当該開示用識別子を漏洩することを抑止するために、通信条件情報 C の部分

に開示用識別子を開示する相手を特定するための情報を記入することができる。このような開示用識別子を生成する場合、c1は"D"として、c2の部分に開示用識別子を開示する相手を特定するための情報、より具体的には開示相手の名前やイニシャルなどを記入することとする。以降の説明では、この形式の開示用識別子を開示先特定型識別子と呼ぶ。

また、通信要求を許可するか拒絶するかをアドレス開示後に動的に設定可能にするため、通信条件情報Cとして、開示用識別子を一意に識別する情報を記入することもできる。具体的には、受信者端末1において開示用識別子を生成する毎に1増加する順序番号を記憶管理することとし、開示用識別子の識別情報を通信条件情報Cに含ませる場合、c1は"I"とし、c2の部分に順序番号を記入する。受信者端末1は、当該端末を使用する受信者に対して、開示済みの開示用識別子を用いて通信要求を許可するか拒絶するか（発信者限定、期限限定、全て拒絶など）を適時設定するインターフェースを提供する。

ところで、上記一連の説明では開示用識別子を生成する際に公開鍵暗号系を用いることとしたが、共通鍵暗号方式を用いることもできる。この具体例をISPのユーザとして企業などの大口顧客がいる場合を想定して説明する。なお、以下の一連の処理はいわゆる共通鍵暗号系にとどまらず、共通する鍵を用いるいかなる暗号系にも適用することができる。

ここでは、中継システムが顧客を一意に識別する顧客名を定義する。例えば、"XXX商事"という企業顧客に対して、"xxx-trading"という顧客名を割り当てる。Step1において、中継システムは、顧客毎に共通鍵を生成し、生成した共通鍵を当該顧客の受信者端末に通知する。また、中継システムは各顧客の顧客名と共通鍵との対応関係を記憶しておく。さらに、Step2において、受信者端末は、NとCとを連結した文字列を共通鍵を用いた共通鍵暗号方式により暗号化し、暗号化結果である文字列に対して、".xxx-trading@gicode.com"というドメイン名を追加して、開示用識別子を生成する。このメールアドレスの@直前のxxx-tradingの部分（ユーザ名部

分) は顧客名を示す文字列となる。

第2図の説明に戻ると、受信者端末1は生成した各開示用識別子を各発信者端末2へ通知する (Step 3)。なお、この通知は電子メールを用いるほか、直接伝えたり、電話、FAX、手紙等のいかなる手段を用いても良い。

5 その後、発信者端末2が前記開示用識別子を指定して中継システム3へ通信を  
要求する (Step 4)。具体的には、発信者端末2はインターネット標準の電子  
メール発信手順に基づき、当該発信者端末2が従属する電子メール中継サーバ  
3bに電子メールを送信する。当該電子メール中継サーバ3bはインターネット  
標準に基づき電子メールを中継する。当該電子メールの宛先の@以降のドメイン  
10 名が"p c o d e . c o m"であるので、当該電子メールはいくつかの電子メール  
中継サーバを経て、電子メール中継サーバ(p c o d e . c o m) 3aへ中継さ  
れる。

そして、中継システム3は、開示用識別子を秘密鍵を用いて復号し、受信者識  
別子及び所定の通信条件情報を取得する (Step 5)。具体的には、電子メー  
15 ルサーバ3aは、受信した電子メールアドレスの宛先の@以前の部分(ユーザ名  
部分)を秘密鍵を用いて復号し、復号結果をStep 2で示した連結子で分離す  
ることにより、N(受信者識別子の@以前の部分)と通信条件情報Cとを取得す  
る。そして、取得したNに"@u s e r . c o m"というドメイン名を追加するこ  
とにより、受信者識別子を取得する。

20 なお、共通鍵暗号方式を用いた場合には、電子メール中継サーバ3aは受信し  
た電子メールアドレスの宛先の@直前の"、"と@との間の文字列を顧客名として  
取得し、当該顧客名に対応する共通鍵を用いて当該電子メールアドレスの先頭か  
ら@直前の"、"までの文字列を復号する。そして、復号後の処理は公開鍵暗号方  
式を用いた方法と同様とする。

25 次に、中継システム3は、受信者識別子または所定の通信条件情報もしくはそ  
の両方にに基づき、通信要求の処理方法を決定する (Step 6)。例えば、通信  
条件情報が受信条件である場合、受信条件を走査し、受信条件が満たされていれ

ば受信者端末1と発信者端末2とを中継、即ち通信確立する。受信条件が満たされていなければ中継を拒否する。なお、ここでいう走査とは、受信条件に関わる情報を収集することを意味する。

具体的には、電子メール中継サーバ3aは、通信条件情報Cの内容に基づき当該電子メールの処理方法を決定する。通信条件情報Cの1文字目が"S"である場合、当該電子メールの発信者アドレスのハッシュ値が通信条件情報Cの2文字目以降に一致することが受信条件となる。また、通信条件情報Cの1文字目が"T"である場合、当該電子メールの受信時刻が通信条件情報Cの2文字目以降よりも以前であることが受信条件となる。また、通信条件情報Cの1文字目が"O"である場合、当該電子メールの発信者アドレスのドメイン名部分のハッシュ値が通信条件情報Cの2文字目以降と一致することが受信条件となる。また、付加条件Cの1文字目が"P"である場合、当該電子メールの発信者アドレスのハッシュ値が通信条件情報Cの2文字目から7文字目までと一致し、かつ、通信条件情報Cの8文字目以降が示す有効期限よりも当該メールの受信時刻が以前であることが受信条件となる。

受信条件が満たされる場合、電子メール中継サーバ3aは、Step 5で取得した受信者識別子を宛先として、当該電子メールを転送する。受信条件が満たされない場合、通信要求を拒絶、即ち当該電子メールを破棄する。

なお、別の処理方法として、受信条件が満たされない場合、予め指定された別のアドレスへ転送することが考えられる。また、別の処理方法として、受信条件が満たされない場合、インターネット掲示板サーバのURLを含む電子メールを発信者へ返信するなど、他の通信形態を選択する形態も考えられる。

また、通信条件情報Cの1文字目が"D"または"I"である場合には、電子メール中継サーバ3aは、通信条件情報Cの文字列を"[Safety Tag="と"]"で囲った文字列を当該電子メールのSubjectフィールドの先頭部に挿入し、受信者識別子を宛先として、当該電子メールを中継する。中継された電子メールはいくつかの電子メール中継サーバ3bを経て、受信者端末へ中継される

。 次に、受信者端末1は通信要求の通知を受信する（Step 7）。通知要求に通信条件情報Cが含まれている場合、当該通信要求を受け付けるか否かを中継システム3へ通知する。具体的には、受信者端末1はIMAPなどの標準プロトコルに基づき、当該端末が従属する電子メール中継サーバ3bから到着メールのリストを、メールのSubjectフィールドを含む形式で受信する。Subjectフィールドの先頭部が”[Safety Tag=”で始まる場合には、”]”までの文字列を通信条件情報Cとして取得し、通信条件情報Cの1文字目が”I”である場合には、通信条件情報Cの2文字目が示す文字列を開示用識別子の順序番号として取得し、当該順序番号について予め受信者が設定した処理方法に基づき処理を行う。

指定された処理が”要求の拒絶”である場合には、受信者端末1は当該メールを削除する指示を電子メール中継サーバ3bに送信する。また、Step 6における中継システムの動作と同様に、別の処理方法として別のアドレスへの転送や別の通信形態の選択（インターネット掲示板の利用）なども考えられる。

なお、通信条件情報Cの種別が識別番号表示”I”または開示先表示”D”のみとし、Step 6において中継システム3は通信要求の処理を判断しないケースや、通信条件情報Cの種別が発信者限定”S”または時間限定”T”のみとし、Step 7において受信者端末1は通信要求の処理を判断しないケースも考えられる。また、通信条件情報Cの種別が開示先表示”D”のみとし、Step 6においてもStep 7においても、中継システム3も受信者端末1も通信要求の処理を判断しないケースも考えられる。

また、開示用識別子を、通信条件情報Cの部分が任意の者に読み取れるように生成するケースも考えられる。このケースでは、Step 2において受信者端末が通信条件情報Cの改竄防止コードを求め、この改竄防止コードとN（受信者識別子の@以前の文字列）とを連結した文字列を公開鍵で暗号化した結果をtとし、このtと通信条件情報Cとを適当な連結子で連結した文字列に”@pcode

．c o m"というドメイン名を追加して開示用識別子を生成する。Step 5においては、電子メール中継サーバ3aが受信した電子メールの宛先の@以前の文字列（ユーザ名）を連結子で分離し、通信条件情報Cとtとを取得する。さらに電子メール中継サーバ3aは、tを秘密鍵で複号し、改竄防止コードとNとを取得する。さらに、電子メール中継サーバ3aは、取得した通信条件情報Cから改竄防止コードを算出した結果とtから取得した改竄防止コードとが一致するかを検査する。簡単な改竄防止コードの具体的な生成方法として、通信条件情報Cのハッシュ値を求める方法が考えられる。

次に、本実施例1をEメールシステムに適用した場合についてさらに具体的に説明する。第3図は、本実施例1に係るメールシステムのシステム構成を示す機能プロック図である。なお、ここでは説明の便宜上、メールを受信する受信者に付与されたメールアドレス（以下、「受信者メールアドレス」と言う）が「a b c @ u s e r . c o m」であり、メールを送信する送信者に付与されたメールアドレス（以下、「送信者メールアドレス」と言う）が「d e f @ u s e r . c o m」であるものとする。また、ここでは説明の便宜上、すでに説明したc1とc2からなる通信条件情報を用いるのではなく、送信者アドレス及び有効期限からなる配送条件情報を用いた場合を示すこととする。また、ここでは共通鍵暗号系を用いるとともに、開示用アドレスを生成する都度受信者アドレスなどを専用ページ上に入力することとする。

同図に示すメールシステムは、送信者端末111の送信者が受信者端末112の受信者に対してメールを送信する際に、受信者の本来のメールアドレスである受信者アドレス「a b c @ u s e r . c o m」をメールの宛先とするのではなく、この受信者アドレスに配送条件情報を埋め込んだ開示用アドレス「S W 6 3 H M 8 v b @ p c o d e . c o m」をメールの宛先として送信する。

これにより、かかるメールは、インターネット110および送信サーバ114を介してドメイン名「p c o d e . c o m」を有するフィルタリングサーバ116に配送され、このフィルタリングサーバ116がメールを受信者に配送すべき

か否かを開示用アドレスに埋め込まれた配送条件情報に基づいて判定し、受信者に配送すべきと判定したもののみについてメールの宛先を受信者アドレス「a b c@user. com」として再配送する。

すると、再配送されたメール118は、インターネット110を介してドメイン名「user. com」を有する受信サーバ115に配送され、受信者アドレス「a b c@user. com」に対応するメールボックス115aに格納されるので、受信者はこのメールボックス115aからメールを取り出すことができる。

このように、かかるメールシステムでは、配送条件情報を埋め込んだ開示用アドレスを宛先アドレスとするメールを送信し、フィルタリングサーバ116において開示用アドレス内の配送条件情報に基づいて適正なものの利用者に配送することにより、配送条件を満たすメールのみを利用者に届けることを可能としている。

次に、第3図に示したメールシステムの構成について説明する。同図に示すように、このメールシステムは、送信者端末111と、受信者端末112と、送信サーバ(SMTPサーバ)114と、受信サーバ(POPサーバ)115と、フィルタリングサーバ116とが、インターネット110に接続されたシステム構成となる。

送信者端末111は、受信者端末112を利用するユーザ(受信者)に対してメールを送信するユーザ(送信者)が利用する端末装置であり、具体的には、受信者端末112向けにメールを送信する際には、該受信者端末112から通知を受けた開示用アドレス「SW63HM8vb@pcode. com」を宛先とし、自身のアドレス「def@user. com」を送信者としたメールを作成してインターネット110に送信する。

受信者端末112は、受信サーバ115内の自身のメールボックス115aからメールを取り出すとともに、自身の開示用アドレスを生成して送信者端末111に通知する処理をもおこなう端末装置であり、配送条件情報取得部112a、

開示用アドレス生成部 112b、開示用アドレス通知部 112c および共通鍵としての暗号鍵を記憶する記憶部 113 を有する。

この配送条件情報取得部 112a は、送信者アドレスおよび／または有効期限（メール配送許可期限）を配送条件情報として取得する処理部であり、たとえば 5、開示用アドレス生成ページにこれらの項目をユーザに入力させることにより該当するデータを取得する。

開示用アドレス生成部 112b は、受信者アドレスおよび配送条件情報（送信者アドレスおよび／または有効期限）に基づいて開示用アドレスを生成する処理部であり、具体的には、受信者アドレスと送信者アドレスの各@以前のユーザ名部（アカウント名）と有効期限からなる文字列を共通鍵を用いて暗号化するとともに、この暗号化データにドメイン名を付与して開示用アドレスを生成する。なお 10、この開示用アドレス生成部 112b の処理は請求項 1 の開示用識別子生成工程に対応し、また、受信者端末 111 が請求項 2 2 の開示用識別子付与装置に対応し、開示用アドレス生成部 112b が請求項 2 2 の開示用識別子生成手段に対応 15 する。

開示用アドレス通知部 112c は、開示用アドレス生成部 112b により生成された開示用アドレスを送信者端末 111 を利用するユーザ（送信者）に通知する処理部であり、具体的には、この送信者の送信者アドレス「d e f @ u s e r . c o m」を宛先とし、開示用アドレス「SW63HM8vb@pcode. c o m」を送信者とする連絡メールによって通知することができる。かかる連絡メールを用いると、送信者は開示用アドレスを入力する必要がなくなるため、入力ミスを防止して円滑なアドレス使用を図ることができる。

記憶部 113 は、あらかじめ受信端末 112 宛に付与された共通鍵としての暗号鍵 113a を暗号鍵の識別情報と対応づけて記憶する記憶デバイスである。この暗号鍵 113a と同じ暗号鍵は、フィルタリングサーバ 116 の配送条件情報抽出処理に必要となるため、フィルタリングサーバ 116 においても保持されて 25 いる。

送信サーバ114は、送信者端末111を利用するユーザ（送信者）がメールを送信する際に用いるSMT Pサーバであり、受信サーバ115は、受信者端末112を利用するユーザ（受信者）がメールを受信する際に用いるP O Pサーバであり、メールボックス115aを有する。なお、このメールボックス115aにメールが到達すると、その旨が受信者端末112に通知され、受信者端末112によるメールボックス115aからのメールの自動受信がおこなわれる。

5 フィルタリングサーバ116は、開示用アドレスに含まれる配送条件情報に基づいて、メールのフィルタリングをおこなうサーバ装置であり、具体的には、配送条件情報に含まれる送信者アドレスとメールの送信者が同一であり、フィルタリングサーバ116によるメール受信時点で配送条件情報に含まれる有効期限が経過していない場合には、当該メールのメールアドレスを本来の受信者アドレス「a b c @ u s e r . c o m」に置き換えて再配送（転送）される。

10 このフィルタリングサーバ116は、メール受信処理部116a、配送条件情報抽出部116b、メール転送処理部116cおよび暗号鍵テーブル116dを有する。なお、この配送条件情報抽出部116bの処理は請求項1の復元工程に対応し、メール転送処理部116cの処理は請求項1の通信確立工程に対応する。また、フィルタリングサーバ116が請求項22の中継システムに対応し、復元部32および中継処理部33がそれぞれ請求項22の復元手段および通信確立手段に対応する。

15 20 メール受信処理部116aは、開示用アドレス「S W 6 3 H M 8 v b @ p c o d e . c o m」を宛先としたメール117を受信する処理部である。かかるフィルタリングサーバ116は、開示用アドレスのドメイン名を有するサーバ装置であるため、すべての開示用アドレスは、このフィルタリングサーバ116によつて受信されることになる。

25 配送条件情報抽出部116bは、メールの宛先をなす開示用アドレスから配送条件情報を抽出する処理部であり、具体的には、開示用アドレス「S W 6 3 H M 8 v b @ p c o d e . c o m」の@前のユーザ名部分「S W 6 3 H M 8 v b」を

暗号鍵を用いて復号化して、受信者アドレスのユーザ名「a b c」、送信者アドレスのユーザ名「d e f」および有効期限「H150701」からなる文字列を抽出し、この送信者アドレスのユーザ名「d e f」に所定のドメイン名「@user.com」を付加した送信者アドレス「def@user.com」および有効期限「H150701」を配送条件情報とする。

ここで、この復号化に用いる暗号鍵は、暗号鍵テーブル116dから取り出すことになるが、フィルタリングサーバ116には様々なメールが到達するため、どの暗号鍵を用いて開示用アドレスを復号化すべきかが不明となる。このため、すでに説明した受信者端末112の開示用アドレス生成部112bで開示用アドレスを生成する段階で暗号鍵の識別IDを付加しておき、この配送条件情報抽出部116bでは、かかる開示用アドレスに含まれる暗号鍵の識別IDを利用して暗号鍵を特定した後、該暗号鍵を用いた復号化をおこなうこととする。

メール転送処理部116cは、配送条件情報抽出部116bにより抽出された配送条件情報に基づいてメールを本来の受信者に転送すべきか否かを判断し、転送すべきものである場合には、開示用アドレスを復号化して得られる受信者アドレスのユーザ名「a b c」に所定のドメイン名「@user.com」を付加した受信者アドレス「a b c@user.com」を宛先としてメールを再配達する。

具体的には、開示用アドレスを復号化して得られる送信者アドレス「def@user.com」がメールの送信者のアドレスと一致する場合には、もともと受信者がメール送信を許可したユーザ（送信者）からのメールであるため、該メールの再配達をすべきものであると判定する。また、メールの受信日時が開示用アドレスを復号化して得られる有効期限「H150701」内であれば、受信者があらかじめ設定した期間内のものであるため、メールの再配達をすべきものであると判定する。

次に、第3図に示した受信者端末112の処理手順についてさらに詳細に説明する。第4図は、第3図に示した受信者端末112の処理手順を示すフローチャ

ートである。この受信者端末 112 では、第 5 図に示す開示用アドレス生成ページ 120 を用いて送信者アドレスおよび有効期限を配送条件情報として取得する (Step 41)。具体的には、この開示用アドレス生成ページ 120 には、受信者アドレスの入力枠 121、送信者アドレスの入力枠 122、有効期限の入力枠 123 が設けられているため、OK の入力枠 124 が指示された際に、これらに入力されたデータのうち送信者アドレスおよび有効期限を配送条件情報として取得すれば良い。

その後、受信者端末 112 は、記憶部 113 に記憶した暗号鍵 113a を取り出し (Step 42)、受信者アドレスおよび送信者アドレスのユーザ名並びに有効期限からなる文字列を暗号鍵 113a で暗号化して開示用アドレスを生成し (Step 43)、生成した開示用アドレスを第 5 図に示す開示用アドレス生成ページ 120 の表示枠 125 に表示するとともに、送信者端末 111 に対して通知することになる (Step 44)。なお、本実施例 1 では、記憶部 113 に記憶する暗号鍵 113a を共通鍵としているため、開示用アドレスを生成する際に共通鍵暗号系の公知の手法を用いれば良い。

次に、第 3 図に示した開示用アドレス生成部 112b による開示用アドレスの生成要領についてさらに具体的に説明する。第 6 図は、第 3 図に示した開示用アドレス生成部 112b による開示用アドレスの生成要領を説明するための説明図である。

同図に示すように、開示用アドレスを生成する際に、まず受信者アドレス「a b c @ u s e r . c o m」の@前のユーザ名部分「a b c」と、送信者アドレス「d e f @ u s e r . c o m」の@前のユーザ名部分「d e f」と、有効期限「H150701」とをブランクで連結した文字列を暗号鍵 113a を用いて暗号化して、暗号化データ「SW63HM8v」を生成する。

その後、この暗号化データに暗号鍵の識別 ID 「b」を付加して「SW63HM8v b」とし、これを開示用アドレスのユーザ名とし、その後にドメイン名「@p c o d e . c o m」を付加して、開示用アドレス「SW63HM8v b @ p

code.com」を生成する。

なお、ここでは説明の便宜上、空白を連結子として用いる場合を示したが、「+」などの文字を連結子として用いることもできる。また、ここでは各メールアドレスのドメイン名が「@user.com」である場合を前提としたため、送信者アドレスと受信者アドレスの@前のユーザ名部分を用いることとしたが、ユーザ名およびドメイン名の全体を暗号化対象とすることもできる。たとえば、「@aaaa.com」、「@bbbb.com」、「@cccc.ne.jp」など様々なドメイン名を持つメールアドレスを処理対象とする場合には、開示用アドレスのデータ長が長くなるものの、ユーザ名およびドメイン名の全体を暗号化対象とする必要がある。

さらに、ここでは説明の便宜上、送信者アドレスおよび受信者アドレスそのものを用いる場合を示したが、送信者アドレスに代えて送信者アドレスのハッシュ値を用い、受信者アドレスに代えて受信者アドレスの圧縮データを用いる場合にも全く同様に適用することができる。

次に、第3図に示したフィルタリングサーバ116の処理手順について説明する。第7図は、第3図に示したフィルタリングサーバ116の処理手順を示すフローチャートである。同図に示すように、このフィルタリングサーバ116では、メール受信処理部116aが開示用アドレスを宛先とするメール117を受信したならば(Step 51)、このメール117から開示用アドレスのユーザ名を取り出すとともに(Step 52)、配送条件情報抽出部116bが暗号鍵データベース116dから該当する暗号鍵を取り出す(Step 53)。

その後、取り出した暗号鍵でユーザ名を復号化して配送条件情報(送信者アドレスおよび有効期限)を取り出し(Step 54)、配送条件情報に含まれる送信者アドレスがメール117の送信者と一致するか否かを確認する(Step 55)。その結果、両者が一致しない場合には(Step 55 No)、本来メール送信が許可されたユーザからのメールではないとみなして、該メール117を破棄するとともに(Step 56)、そのログを記録する(Step 57)。

一方、配送条件情報に含まれる送信者アドレスがメール117の送信者とが一致する場合には（Step 51 Yes）、メール117の受信日時が配送条件情報に含まれる有効期限内であるか否かを調べる（Step 58）。その結果、有効期限内ではない場合には（Step 58 No）、期限超過を理由として該メール  
5 117を破棄するとともに（Step 56）、そのログを記録し（Step 57）、有効期限内である場合には（Step 58 Yes）、いずれの条件をも満たすとみなして、メール117の宛先を本来の受信者アドレスに変更してメール117を転送する（Step 59）。

次に、第3図に示した配送条件情報抽出部116bおよびメール転送処理部116cによるフィルタリングの実施要領についてさらに具体的に説明する。第8図は、第3図に示した配送条件情報抽出部116bおよびメール転送処理部116cによるフィルタリングの実施要領を説明するための説明図である。

同図に示すように、メール117の宛先である開示用アドレス「SW63HM8vb@pcode.com」からユーザ名部分「SW63HM8vb」を取り出し、この末尾に位置する暗号鍵の識別ID「b」を用いて暗号鍵テーブル116dから該当する暗号鍵を抽出する。

その後、抽出した暗号鍵を用いて「SW63HM8v」を復号化し、「abc def H150701」の文字列を取得し、この「abc」にドメイン名「@user.com」を付加したアドレス「abc@user.com」を受信者アドレスとし、「def」にドメイン名「@user.com」を付加したアドレス「def@user.com」を送信者アドレスとし、「H150701」を有効期限とする。

その後、メール117の送信者が「def@user.com」である場合には、送信者の条件を満たすものと判定し、メール117の受信日時が「H150701」以前であれば、時期的条件を満たすものと判定する。そして、両者の条件を満たす場合には、開示用アドレスから取り出した「abc@user.com」をメール117の受信者アドレスとしてメールを転送し、いずれか一つでも

条件を満たさない場合には、メールを破棄してログを記録する。

なお、ここでは説明の便宜上、条件を満たさない場合にメールを破棄することとしたが、条件を満たさない場合に管理者などのメールアドレスを宛先アドレスとして転送することもできる。このようにすれば、管理者などが迷惑メールなどの状況を適宜把握することができる。

このように、受信者端末112の開示用アドレス生成部112bにより受信者アドレスと配送条件情報を暗号化して開示用アドレスを生成して送信者端末111に通知し、送信者端末111から送信された開示用アドレスを宛先とするメール117をフィルタリングサーバ116で受信したならば、配送条件情報抽出部116dが開示用アドレスから配送条件情報を抽出し、配送条件情報の条件を満たす場合にのみ本来の受信者アドレスにメールを転送するよう構成することにより、受信者アドレスの漏洩および拡散に伴う該受信者アドレスの用途外使用を抑制することができる。なお、ここでは説明の便宜上、共通鍵暗号系を用いた場合を示したが、すでに説明したように公開鍵暗号系を用いた場合に適用することもできる。また、ここで言う受信者端末とは、受信者が使用するコンピュータ、ルータ、P BXなどを含むものとする。

#### (実施例2)

ところで、上記一連の説明では、開示用識別子の生成及び通知を受信者端末でおこなうこととしたが、開示用識別子付与装置として受信者端末を用いた場合には、受信者自身が発信者毎、またはその都度、開示用識別子を生成し、通知しなければならず、煩わしいという問題がある。また、発信者は当然、受信者識別子を知らないから、開示用識別子を要求するに当たって前述した中継システムを利用した通信以外の別の手段で受信者に開示用識別子を求める必要がある。また、開示用識別子を発信者へ通知する時も、通信形態によっては受信者の受信者識別子が発信者側に知られる恐れがあるため、別の手段で通知することが必要になる場合もある。

ここで、開示用識別子付与装置として受信者端末以外の装置、例えば受信者端

末及び中継システムのいずれとも異なる仲介装置を用いると、受信者が開示用識別子を生成し、通知する煩わしさがなくなり、また、発信者は通信により開示用識別子を要求し、受領することが可能となる。そこで、以下では仲介装置において開示用識別子の生成及び通知を行う場合について説明する。

5 第9図は、開示用識別子付与装置として仲介装置4を用いた場合の本発明の通信システムの基本構成を示す図である。中継装置4は、第1図に示した受信者識別子記憶部11、開示用識別子生成部12及び開示用識別子通知部13とそれぞれ基本的に同一の受信者識別子記憶部41、開示用識別子生成部42及び開示用識別子通知部43を備える外、発信者の通信端末からの受信者の開示用識別子の開示要求を受け付ける識別子要求受付部44を備えている。

かかる構成において、発信者端末2は、仲介装置4に対して受信者端末1の開示用識別子の開示を通常の中継システム（図示せず）を用いた通信によって要求する。仲介装置4において、識別子要求受付部44がこの要求を受信すると、開示用識別子生成部42は受信者識別子記憶部41に記憶された受信者識別子Rと、別途記憶されもしくは入力された所定の通信条件情報Cとから、中継システム3の運用者以外も実行可能な方法で開示用識別子Tを生成し、開示用識別子通知部43より通常の中継システムを用いた通信によって発信者端末2へ通知（開示）する。

この際、仲介装置4に、受信者の開示用識別子の開示を要求する発信者がその資格を有するか否かを判断し、資格がない場合は当該要求を棄却する認証部45を設けておけば、受信者にとって迷惑な通信を企む第三者に対して本仲介装置4が開示用識別子を開示することを防ぐことができる。

発信者端末2は、開示用識別子Tを指定して中継システム3に通信を要求する。以後の動作は第1図の場合と同様である。なお、受信者識別子記憶部41には、予め受信者端末1もしくは中継システム3より通常の中継システムを用いた通信によって送られた受信者識別子Rが記憶されているものとする。

第10図は、仲介装置が即ち開示用識別子の生成及び通知をおこなう場合の処

理手順を示すシーケンス図である。すでに実施例1で説明したように、あるISPが本発明に基づく電子メール中継システムを運用していることを前提とし、ある会社IDPが自社の顧客をISPに会員登録しており、提携EC業者に対して顧客の開示用識別子を開示する。IDPの顧客は、IDPによって割り当てられた顧客IDを持ち、ISPが運用する電子メール中継サーバ3b上に電子メールアカウントを持ち、“顧客名@user.com”という形式の電子メールアドレスを持つ。

提携EC業者は、会社IDPの顧客がWEBブラウザで商品を注文することを可能にするECサイトを運営する。提携EC業者は、商品の注文と同時に顧客のWEB端末が当該顧客の顧客IDをECサイトのサーバへ送信するようにECサイトの注文ページを構成する。このような注文ページは、標準のHTMLにより記述可能である。この場合、注文情報は標準のHTTP手順によりECサイトへ送信される。

会社IDPは、仲介装置4としてWEBサーバを設置する。このWEBサーバは会社IDPの各顧客について、当該顧客の顧客IDと電子メールアドレスとを記憶するアドレスデータベースを備える。このようなアドレスDBは市販のリレーショナルデータベースソフトを用いて実現できる。

まず、HTTPプロトコルにもとづくフォーム送信手順などを用いて、会社IDPの顧客は自身の電子メールアドレスを会社IDPの仲介装置4に登録した後(Step11)、ISPは秘密鍵と公開鍵を用意し、公開鍵を公開する(Step12)。なお、共通鍵を用いて条件付き受信者識別子を生成する場合には、ISPは会社IDPを一顧客として、会社IDPに対応する共通鍵を生成して会社IDPへ通知する。

その後、会社IDPの顧客がWEB端末を用いて、提携EC業者のECサイトのホームページを閲覧し、商品を注文する(Step13)。これにより、WEB端末は当該顧客の顧客IDを含む注文情報をECサイトのサーバに送信し、ECサイトのサーバは注文情報を受信する。

その後、ECサイトのサーバは、受信した注文情報から顧客IDを取得し、顧客IDを含むアドレス開示要求を仲介装置4へ送信する（Step 14）。具体的には、顧客IDを検索キーとして含むHTTP要求メッセージをHTTPプロトコルに基づき送信する。また、ECサイトのサーバは、自身の認証情報をHTTP要求メッセージに含ませる。

その後、仲介装置4はアドレス開示要求を受信し、要求の送信元が提携業者の装置であるか認証し、さらに要求に含まれるIDを取得する（Step 15）。この認証は、HTTPプロトコルにもとづくベーシック認証やダイジェスト認証により実現することができる。要求の送信元が提携業者の装置でない場合には要求を棄却する。要求の送信元が提携業者の装置である場合には以下の手順を実行する。

すなわち、仲介装置4はStep 14において取得した顧客IDに対応する顧客の電子メールアドレスをアドレスDBを参照して取得するとともに、この電子メールアドレスを受信者識別子として、実施例1のStep 2に示した手順により開示用識別子を生成する（Step 16）。

公開鍵を用いて開示用識別子を生成する場合には、仲介装置4はISPが公開する公開鍵を使用し、共通鍵を用いて開示用識別子を生成する場合には、仲介装置は当該IDPの共通鍵を使用する。

条件として、発信者アドレスを限定する情報または開示用識別子の有効期限を指定する情報を含ませることができる。発信者アドレスを限定する場合には、仲介装置4は提携業者の電子メールアドレスを記憶するDBを持つこととし、実施例1のStep 2に示したc1を“S”とし、Step 15で認証した要求送信元の電子メールアドレスのハッシュ値をc2とする。一方、有効期限を指定する場合には、c1を“T”として当該時点から一定時間（14日間、30日間など）を加算した値をc2とする。

その後、仲介装置4は、生成した開示用識別子を含ませて、アドレス開示要求に対する応答メッセージをECサイトのサーバへ送信し（Step 17）、EC

サイトのサーバは、受信した条件付き受信者識別子を Step 13 で受信した注文情報とともに記憶する (Step 18)。

5 提携 EC 業者の従業員は、必要に応じて前記顧客に対して電子メールで連絡をとる。この際、EC サイトが Step 18 で記憶した条件付き受信者識別子を電子メールの宛先として電子メールを送信する。以降の動作は実施例 1 の Step 4 以降と同様の処理となる。このようにして電子メールアドレスを流通させれば、EC 業者の従業員が顧客の電子メールアドレスを不当な目的で漏洩させることを防ぐことができる。

10 次に、本実施例 2 を E メールシステムに適用した場合についてさらに具体的に説明する。第 11 図は、開示用アドレスの生成とフィルタリングの両方をおこなう開示用メール処理サーバ 132 を設けた場合のシステム構成を示す図である。

15 同図に示すように、この場合には、受信者端末 130 では配送条件情報取得部 112a により配送条件情報を取得したならば、アドレス通知依頼部 131 により開示用アドレスを送信者端末 11 に通知するよう開示用メール処理サーバ 132 に依頼することになる。具体的には、このアドレス通知依頼には、受信者アドレスおよび配送条件情報（送信者アドレスおよび有効期限）を含める必要がある。

20 開示用メール処理サーバ 132 のアドレス通知処理部 133 に含まれるアドレス通知依頼受付部 133a が、受信者端末 130 からかかるアドレス通知依頼を受け付けたならば、開示用アドレス生成部 133b が開示用アドレスを生成し、開示用アドレス通知部 133c が開示用アドレスを送信者端末 11 に通知する。なお、フィルタリング処理部 134 を形成するメール受信処理部 134a、配送条件情報抽出部 134b およびメール転送処理部 134c は、第 3 図に示したフィルタリングサーバ 116 のメール受信処理部 116a、配送条件情報抽出部 116b およびメール転送処理部 116c と同様の機能を有する。

25 このように、開示用アドレスの生成を受信者端末 130 とは別のサーバ装置におこなわせることにより、受信者端末 130 の処理負荷増を招くことなく、開示

用アドレスの生成をおこなうことができる。特に、第11図に示すように、開示用アドレスの生成とフィルタリングを同じサーバ装置におこなわせることにより、開示用アドレスの処理を一元化することができるため、単独の業務サービスとして提供するビジネス形態を採用する場合に有利となる。

5 (実施例3)

ところで、上記実施例2では仲介装置に受信者識別子を登録する場合を示したが、受信者が仲介装置の運用者にも受信者識別子を知られたくない場合がある。このような場合、受信者の通信端末または中継システムにおいて受信者の受信者識別子R及び特定の情報（仮通信条件情報）C○を用いて仮の開示用識別子T○を生成し、この仮の開示用識別子T○を受信者の受信者識別子として仲介装置に登録し、仲介装置では別の装置に特定の付加情報C○を本来の通信条件情報Cに書き換えることを依頼して仮開示用識別子T○から開示用識別子Tを得て、この開示用識別子Tを発信者に対して通知する。

15 第12図は、識別子書換装置5を用いた本発明の通信システムの基本構成を示す図である。同図に示すように、この開示用識別子書換装置5は、書換要求受付部51、復元部52、開示用識別子生成部53及び応答部54を有する。

かかる構成において、受信者端末1は、予めその受信者識別子R及び特定の情報、特に開示先を仲介装置4に限定する情報（仮通信条件情報）C○を用いて仮開示用識別子T○を生成し、通常の中継システムを用いた通信によって仲介装置20 4に送り、受信者識別子記憶部41に登録する。

発信者端末2は、仲介装置4に対して受信者端末1の開示用識別子の開示を通常の中継システム（図示せず）を用いた通信によって要求する。仲介装置4において、識別子要求受付部44がこの要求を受信すると、開示用識別子生成部42は受信者識別子記憶部41に記憶された仮の開示用識別子T○と、別途記憶され25 もしくは入力された所定の通信条件情報Cとを指定して、開示用識別子書換装置5に通常の中継システムを用いた通信によって通信条件情報の書き換えを要求する。

開示用識別子書換装置 5において、書換要求受付部 5 1がこの要求を受信すると、復元部 5 2は書換装置 5 の運用者のみが実行可能な方法で仮開示用識別子 T oを復号して受信者識別子 R と特定の仮通信条件情報 C oを取得する。開示用識別子書換装置 5 の開示用識別子生成部 5 3は取得した受信者識別子 R と指定された通信条件情報 C oとから、中継システム 3 の運用者以外も実行可能な方法で開示用識別子 T を生成し、応答部 5 4により通常の中継システムを用いた通信によって中継装置 4へ送信する。

この際、開示用識別子書換装置 5 に、書き換えを要求する仲介装置がその資格を有するか否かを仮開示用識別子 T oの仮通信条件情報、即ち開示先を仲介装置 4に限定する情報 C oに基づいて判断し、資格がない場合は当該要求を棄却する認証部 5 5を設けておけば、受信者にとって不適格な仲介装置に対して本開示用識別子書換装置 5 が仮通信条件情報の書き換えを行うことを防ぐことができる。

中継装置 4は、受信した開示用識別子 T を開示用識別子通知部 4 3により通常の中継システムを用いた通信によって発信者端末 2 へ送信する。発信者端末 2 は、開示用識別子 T を指定して中継システム 3 に通信を要求する。以後の動作は第 1 図の場合と同様である。

第 1 3 図は、実施例 3 の処理手順を示すシーケンス図である。ここでは、ISP は開示用識別子書換装置 5 を運用する。ISP は IDP に対して仲介業者 ID を割り当てるこことし、顧客は仮開示用識別子 T oの生成において、通信条件情報 C oとして仲介業者 ID を有する開示先特定型識別子を生成する。さらに、顧客は実施例 2 の Step 1 1において、自身の電子メールアドレスの代わりに開示先特定型識別子を仲介装置 4 に通知する。そして、実施例 2 の Step 1 6 の動作は以下の通りとなる。

まず、仲介装置 4 は、Step 1 5 で取得した顧客 ID に対応する顧客の電子メールアドレスを、アドレス DB を参照して取得する。そして、この電子メールアドレスが仮開示用識別子の形式であった場合には、当該電子メールアドレス T oと所定の仮通信条件情報 C oとを含む書き換え要求を開示用識別子書換装置 5 へ

送信する (Step 21)。具体的には、電子メールアドレス  $T_0$  と仮通信条件情報  $C$  を含む HTTP 要求メッセージを送信する。この際、仲介業者 ID を含む認証情報を要求メッセージに含ませる。ここで、 $C$  は、EC サイトに発信者を限定する情報とする。即ち、 $c_1$  を "S" とし、 $c_2$  は EC サイトの電子メールアドレスのハッシュ値とする。

その後、書換装置 5 は HTTP 要求メッセージを受信し、実施例 1 の Step 5 と同様にアドレス  $T_0$  から受信者識別子  $R$  と仮通信条件情報  $C_0$  とを取得し、仮通信条件情報  $C_0$  と要求メッセージに含まれる認証情報が示す仲介業者 ID とが一致するか検査する。一致する場合には、受信者識別子  $R$  と新しい通信条件情報  $C$  とから、実施例 1 の Step 2 と同様にして開示用識別子  $T$  を生成する (Step 22)。なお、一致しない場合には、当該書き換え要求を棄却する。

その後、書換装置 5 は、要求メッセージに対する応答として開示用識別子  $T$  を仲介装置 4 に対して送出する (Step 23)。

なお、本実施例 3 では、受信者端末で仮開示用識別子を生成することとしたが、ここで言う受信者端末とは、受信者が使用するコンピュータ、ルータ、PBX などを含むものとする。また、受信者の通信端末のほか、受信者識別子を付与する中継システムで開示用識別子及び仮の開示用識別子を生成するようになしても良い。

#### (実施例 4)

ところで、上記実施例 1 ~ 3 では、メールシステムに本発明を適用する場合を示したが、本発明はメールシステム以外にも適用することができる。そこで、本実施例 4 では、本発明を電話交換システム（電話番号）に適用した場合を示すこととする。

まず、本実施例 4 に係る電話交換システムの特徴について説明する。第 14 図は、本実施例 4 に係る電話交換システムのシステム構成を示す機能ブロック図である。なお、本実施例 4 では、電話機から電話をおこなった際に、相手の電話番号と自身の電話番号が相手側に通知されるものとする。

同図に示す電話交換システムは、発信者用電話機 141 のユーザ（発信者）が着信者用電話機 142 のユーザ（着信者）に電話をおこなう際に、単に着信者用電話機 142 の電話番号をダイヤリングするのではなく、通話条件情報を埋め込んだ開示用電話番号をダイヤリングする。具体的には、かかる電話番号は、たとえれば 0132-111-111 というサービス特番を含む電話番号とし、電話が開示用電話番号処理装置 143 向けとなるようにする。

これにより、かかる電話は、開示用電話番号処理装置 143 においてオフフックされ、開示用電話番号に含まれる通話条件情報に基づいて発信者用電話機 141 と着信者用電話機 142 との間の通話回線を接続すべきか否かが判定され、接続すべきと判定された場合には、この開示用電話番号処理装置 143 から着信者用電話機 142 にダイヤリングするとともに、交換機 B に対して発信者用電話機 141 と着信者用電話機 142 との間の通話回線を接続するよう指示する。

このように、かかる電話交換システムでは、通話条件情報を埋め込んだ開示用電話番号を用いて発信者用電話機 141 から開示用電話番号処理装置 143 に対してダイヤリングし、この開示用電話番号処理装置 143 が開示用電話番号内の通話条件情報に基づいて適正なもののみを回線接続することにより、通話条件を満たす通話要求のみを回線接続することとしている。

次に、第 14 図に示した電話交換システムの構成について説明する。同図に示すように、この電話交換システムは、電話交換網 140 を形成する交換機 A に発信者用電話機 141 が接続され、交換機 B に開示用電話番号処理装置 143 が接続され、交換機 C に着信者用電話機 142 が接続されたシステム構成となる。そして、これらの交換機 A、B および C は、サービス特番「0132-111-111」の電話番号を受け付けた場合に、開示用電話番号処理装置 143 に回線接続するものとする。

ここで、この開示用電話番号処理装置 143 は、開示用電話番号の生成および該開示用電話番号に含まれる通話条件情報に基づくフィルタリングをおこなう装置であり、電話番号通知処理部 144 と、フィルタリング処理部 145 と、暗号

鍵テーブル 1 4 6 とを有する。

電話番号通知処理部 1 4 4 は、着信者用電話機 1 4 2 から開示用電話番号の通知要求を受け付けた際に、着信電話番号と通話条件情報に基づいて開示用電話番号を生成して発信者用電話機 1 4 1 に通知する処理部であり、開示用電話番号通知要求受付部 1 4 4 a、通話条件情報取得部 1 4 4 b、開示用電話番号生成部 1 4 4 c および開示用電話番号通知部 1 4 4 d を有する。

開示用電話番号通知要求受付部 1 4 4 a は、着信者用電話機 1 4 2 からの発信者用電話機 1 4 1 に対する開示用電話番号の通知要求を受け付ける処理部であり、具体的には、自動音声応答による番号入力により開示用電話番号の通知要求を確認する。

通話条件情報取得部 1 4 4 b は、開示用電話番号に埋め込む通話条件情報を取得する処理部であり、具体的には、自動音声応答により通話条件情報をなす送信者電話番号と有効期限を取得して、開示用電話番号生成部 1 4 4 c に出力する。

開示用電話番号生成部 1 4 4 c は、着信電話番号および通話条件情報（発信電話番号および有効期限）に基づいて開示用電話番号を生成する処理部であり、具体的には、着信電話番号、発信電話番号、有効期限がらなる文字列を共通鍵暗号系の暗号鍵で暗号化した暗号化データに暗号鍵の識別 ID を付与するとともに、これにサービス特番「0132-111-111」を附加して開示用電話番号とする。

開示用電話番号通知部 1 4 4 d は、開示用電話番号生成部 1 4 4 c により生成された開示用電話番号を発信者用電話機 1 4 1 に通知する処理部であり、具体的には、自動ダイヤリングおよび音声メッセージを用いて開示用電話番号を通知する。

フィルタリング処理部 1 4 5 は、開示用電話番号に含まれる通話条件情報（通話条件）に基づいて着信者用電話機 1 4 2 と発信者用電話機 1 4 1 との間の回線接続をおこなうか否かを判定し、通話条件を満たす場合にのみ回線接続をおこなう処理部であり、着信受付部 1 4 5 a、通話条件情報抽出部 1 4 5 b および回線

接続指示部 145c を有する。

着信受付部 145a は、発信者用電話機 141 からの開示用電話番号を用いた着信を受け付ける処理部であり、通話条件情報抽出部 145b は、開示用電話番号から通話条件情報を暗号鍵で復号化して発信電話番号および有効期限を取り出す処理部である。

回線接続指示部 145c は、通話条件情報抽出部 145b により抽出された発信者電話番号が正当なものであり、かつ有効期限を超過していない場合に、着信者用電話機 142 にダイヤリング（発呼）するとともに、着信者用電話機 142 と発信者用電話機 141 の間を回線接続するよう交換機 B に指示する処理部である。

10

次に、第 14 図に示した着信者用電話機 142、開示用電話番号処理装置 143 および発信者用電話機 141 の処理手順について説明する。第 15 図は、第 14 図に示した着信者用電話機 142、開示用電話番号処理装置 143 および発信者用電話機 141 の処理手順を示すシーケンス図である。

15

同図に示すように、まず着信者用電話機 142 を利用するユーザ（着信者）が、通信販売申込み用の開示用電話番号が必要になったような場合に、開示用電話番号処理装置 143 の電話番号「0132-111-111」をダイヤルして回線接続要求をおこなうとともに（Step 61）、音声ガイダンスにしたがって通話条件情報を送出する（Step 62）。具体的には、発信電話番号（通信販売業者のメールアドレス）と有効期限を通話条件情報として送出することになる

20

。そして、開示用電話番号処理装置 143 が、かかる通話条件情報を取得したならば、この通話条件情報を埋め込んだ開示用電話番号を生成し（Step 63）、生成した開示用電話番号を発信者用電話機 141 のユーザに音声メッセージにより通知する（Step 64）。

25 その後、発信者用電話機 141 のユーザが開示用電話番号の一部「0132-111-111」をダイヤルして回線接続要求をおこなった後に（Step 65）

5 ) 、開示用電話番号の残余の部分をなす付加番号を開示用電話番号処理装置 14 3 に送信すると (Step 66) 、開示用電話番号処理装置 14 3 では、付加番号を復号化して通話条件情報を抽出し (Step 67) 、この通話条件情報に基づいて回線接続の可否を判定し (Step 68) 、通話条件情報の通信条件を満たす場合には、着信者用電話機 14 2 と発信者用電話機 14 1 との間の回線接続をおこなう (Step 69) 。

10 次に、第 14 図に示した電話番号通知処理部 14 4 の処理手順について説明する。第 16 図は、第 14 図に示した電話番号通知処理部 14 4 の処理手順を示すフローチャートである。同図に示すように、開示用電話番号通知要求受付部 14 4 a が着信者用電話機 14 2 からの開示用電話番号の通知要求を受け付けると (Step 71) 、通話条件情報取得部 14 4 b は音声ガイダンスをおこなって、着信電話番号、発信電話番号および有効期限を順次受け付ける (Step 72 ~ 74) 。

15 その後、暗号鍵テーブル 14 6 から暗号鍵を取り出し (Step 75) 、着信電話番号、発信電話番号および有効期限からなる文字列を暗号鍵で暗号化して付加番号を生成するとともに (Step 76) 、この付加番号に暗号鍵の識別 ID を付加し (Step 77) 、さらにこの付加番号にサービス特番「0132-11-111」を付加して (Step 78) 、開示用電話番号を生成し、生成した開示用電話番号を発信者用電話機 14 1 のユーザに対して通知する (Step 79) 。

20 次に、第 14 図に示した開示用電話番号生成部 14 4 c による開示用電話番号の生成要領についてさらに具体的に説明する。第 17 図は、第 14 図に示した開示用電話番号生成部 14 4 c による開示用電話番号の生成要領を説明するための説明図である。

25 同図に示すように、開示用電話番号を生成する際に、まず着信電話番号「03 - 1234-5678」と、発信電話番号「0422-11-2222」と、有効期限「H150701」とをブランクで連結した文字列を暗号鍵「A12xy」

z」を用いて暗号化して、暗号化データ「536289013250069824」を生成する。

その後、この暗号化データに暗号鍵の識別ID「#58」を付加して付加番号

「536289013250069824#58」とし、これにサービス特番「

5 0132-111-111」を付加した「0132-111-111 5362

89013250069824#58」を開示用電話番号とする。

なお、すでに説明したように「+」などの文字を連結子として用いることでも  
きる。また、電話番号全体を使って付加番号を生成するのではなく、市内局番以  
降（たとえば、03-1234-5678の場合には、「12345678」）  
10 を用いて付加番号を生成することもできる。

次に、第14図に示したフィルタリング処理部145の処理手順について説明  
する。第18図は、第14図に示したフィルタリング処理部145の処理手順を  
示すフローチャートである。同図に示すように、このフィルタリング処理部14  
5では、着信受付部145aが開示用電話番号の着信を受け付けたならば（S t  
ep 8 1）、通話条件情報抽出部145bが暗号鍵テーブル146から該当する  
15 暗号鍵を取り出す（S t e p 8 2）。

その後、取り出した暗号鍵で付加番号を復号化して通話条件情報（発信電話番  
号および有効期限）を取り出し（S t e p 8 3）、通話条件情報に含まれる発信  
電話番号が発信通知された発信元の電話番号と一致するか否かを確認する（S t  
ep 8 4）。その結果、両者が一致しない場合には（S t e p 8 4 N o）、許可  
20 されたユーザからの電話ではないとみなして、通話を切断するとともに（S t e  
p 8 5）、そのログを記録する（S t e p 8 6）。

一方、通話条件情報に含まれる発信電話番号が発信通知された発信元の電話番  
号と一致する場合には（S t e p 8 4 Y e s）、着信日時が通話条件情報に含ま  
25 れる有効期限内であるか否かを調べる（S t e p 8 7）。その結果、有効期限内  
でない場合には（S t e p 8 7 N o）、期限超過を理由として通話を切  
断するとともに（S t e p 8 5）、そのログを記録し（S t e p 8 6）、有効期限内である  
もに（S t e p 8 5）、そのログを記録し（S t e p 8 6）、有効期限内である

場合には（Step 87 Yes）、いずれの条件をも満たすとみなして、着信者用電話機142に電話連絡するとともに、交換機Bに対して回線接続をするよう指示する（Step 88）。

次に、第14図に示した通話条件情報抽出部145bおよび回線接続指示部145cによるフィルタリングの実施要領についてさらに具体的に説明する。第15図は、第14図に示した通話条件情報抽出部145bおよび回線接続指示部145cによるフィルタリングの実施要領を説明するための説明図である。

同図に示すように、開示用電話番号の付加番号「5362890132500 69824 #58」の末尾に位置する暗号鍵の識別ID「#58」から暗号鍵を特定して暗号鍵テーブル146から該当する暗号鍵を取り出し、該暗号鍵で付加番号「536289013250069824」を復号化する。

これにより、「0312345678 0422112222 H150701」という文字列が得られるため、本電話の発信元の電話番号が「0422-11-2222」であるか否かを調べ、また着信日時が「H15.07.01」以前であるか否かを調べる。

そして、両者の条件を満たす場合には、着信電話番号を持つ着信者用電話機142と発信者用電話機141との間を回線接続し、いずれか一つでも条件を満たさない場合には、通話を切断してログを記録する。

なお、ここでは説明の便宜上、条件を満たさない場合に通話を切断することとしたが、条件を満たさない場合に管理者などの電話機との間で回線接続することもできる。このようにすれば、管理者などが迷惑電話などの状況を適宜把握することができる。

このように、開示用電話番号処理装置143の開示用電話番号生成部144Cにより着信電話番号と通話条件情報を暗号化して開示用電話番号を生成して発信者用電話機141に通知し、発信者用電話機141から開示用電話番号による通信接続要求を受け付けたならば、通話条件情報抽出部145bが開示用電話番号に含まれる付加番号から通話条件情報を抽出し、通話条件情報の条件を満たす場

合にのみ着信者用電話機142との間の回線接続をおこなうよう構成することにより、着信電話番号の漏洩および拡散に伴う該着信電話番号の用途外使用を抑制することができる。

なお、ここでは通話条件情報（通話条件）として発信者電話番号および有効期限を用いた場合を示したが、いずれか一方を通話条件情報とすることもでき、これら以外の条件を通話条件情報とすることもできる。また、共通鍵暗号系ではなく公開鍵暗号系を用いた場合に適用することもできる。

また、ここでは説明の便宜上、着信者用電話機142から音声ガイダンスを利用して開示用電話番号の通知を依頼する場合を示したが、インターネット上のWEBサーバを利用して開示用電話番号の通知を依頼することもできる。第20図は、インターネット上のWEBサーバを利用して開示用電話番号の通知を依頼する場合のシステム構成を示す図であり、同図に示すように、着信者用端末161から開示用電話番号の通知依頼をおこなうと、開示用電話番号通知サーバ163が開示用電話番号を生成して発信者用端末162に通知するものである。この際、第21図に示すように、開示用電話番号通知サーバ163から着信者用端末161に対して開示用電話番号生成ページ170を提供し、着信電話番号の入力枠171、発信電話番号の入力枠172、有効期限の入力枠173にデータを入力してOKの入力枠174を指示することにより、開示用電話番号の表示枠175に開示用電話番号を表示するとともに、この開示用電話番号を発信者用端末162に通知することができる。

ところで、上記実施例1～4では、システム構成を機能ブロック図として示したが、各装置はプログラムで動作するコンピュータを用いて実現することができる。第22図は、第3図に示したフィルタリングサーバ16のハードウェア構成を示すブロック図である。同図に示すように、かかるフィルタリングサーバ11は、ディスプレイ181、キーボード182、RAM183、HDD184、HD185、ROM186およびCPU187をバス188で接続した構成となる。HD185には、暗号鍵テーブル185a、メール転送プログラム185b

、通信条件情報抽出プログラム 185c およびメール受信プログラム 185d が  
格納されており、この暗号鍵テーブル 185a が RAM 183 上に読み込まれて  
第3図の暗号鍵テーブル 16d として機能する。また、メール転送プログラム 1  
85b、通信条件情報抽出プログラム 185c およびメール受信プログラム 18  
5d は、メール転送プロセス 187c、通信条件情報抽出プロセス 187b およ  
びメール受信プロセス 187a として CPU 187 上で動作実行する。このメー  
ル転送プロセス 187c が第3図のメール受信処理部 16a に対応し、通信条件  
情報抽出プロセス 187b が第3図の通信条件情報抽出部 16b に対応し、メー  
10 ル受信プロセス 187a が第3図のメール転送処理部 16c に対応することにな  
る。なお、ここでは説明の便宜上、第3図のフィルタリングサーバ 116 につい  
てのみ説明したが、他の装置についても同様のハードウェア構成を前提として機  
能する。

なお、これらのメール転送プログラム 185b、通信条件情報抽出プログラム  
185c およびメール受信プログラム 185d は、HD 185 から CPU 187  
15 にロードする場合だけではなく、CD-R などの記録メディアからロードしても  
良い。たとえば、CD-R からプログラムをロードする場合には、あらかじめこ  
れらのメール転送プログラム 185b、通信条件情報抽出プログラム 185c お  
よびメール受信プログラム 185d などを CD-R に格納しておき、この CD-  
R を図示しない CD-R 読取装置に装着して各プログラムをロードすることにな  
20 る。

なお、第23図は実施例1における受信者端末をコンピュータ上で実現するプ  
ログラムを示す動作の流れ図であり、第24図は実施例1～3における中継シス  
テムをコンピュータ上で実現するプログラムを示す動作（但し、開示用識別子を  
指定した通信要求を受信した以後のみ）の流れ図であり、第25図は実施例2に  
25 における仲介装置をコンピュータ上で実現するプログラムを示す動作の流れ図であ  
り、第26図及び第27図はそれぞれ実施例3における仲介装置及び開示用識別  
子書換装置をコンピュータ上で実現するプログラムを示す動作の流れ図である。

以上、電子メール通信サービスおよび電話交換システムへ本発明を適用した場合について説明したが、本発明はIP電話サービスへ適用することもできる。このためには、上記実施例1における電子メールアドレスに対する処理と同様の開示用識別子の生成、復元処理をIP電話における受信者識別子であるSIP URIに適用する。さらに、上記実施例1における電子メールの処理と同様の通信要求処理をIP電話における通信要求メッセージであるSIP INVITEメッセージに対して適用することになる。

(実施例5)

第28図は、本実施例5に係るメール配送システムのシステム構成を示す図である。同図に示すメール配送システムは、着信者端末B220と発信者端末B320とを着側IP網B200、発側インターネットB400および発側IP網B300を介して接続し、この発信者端末B320から発信された着信者B230の着信者アドレスを宛先としたメールを着信者端末B220まで配送するメール配送システムである。

ここで、このメール配送システムは、着信者B230に配送するメールの配送条件を示す配送条件情報（コンテキスト情報）と着信者アドレスに基づいて開示用のアドホックアドレスを発行するアドホックアドレス発行サーバB120と、かかるアドホックアドレスを宛先とするメールを着信した際に、該アドホックアドレスから着信者アドレスの復元およびコンテキスト情報の抽出をおこない、該抽出したコンテキスト情報に含まれる配送条件を当該メールが満たす場合に、該メールの宛先をアドホックアドレスから復元した着信者アドレスに置き換えて当該メールを転送するアドホックメール転送サーバB110とを設けたことを特徴とする。ここで、「着信者アドレスの復元」には、アドホックアドレスを復号化して直接着信者アドレスを復元する場合のほか、後述する実施例7において言及するアドレステーブルを用いてアドレス識別子を介して復元する場合も含まれる。また、「コンテキスト情報の抽出」とは、アドホックアドレスからコンテキスト情報をデータ列として抽出する場合のほか、アドホックアドレスを暗号化技術

により復号化してコンテキスト情報を抽出する場合も含まれる。

すなわち、このメール配達システムでは、着信者B230が保有する着信者アドレスそのものを宛先として発信者端末B320から着信者端末B220に向けてメールを転送するのではなく、開示用のアドホックアドレスを用いてメールを転送することとしている。かかるアドホックアドレスを用いる理由は、着信者B230が発信者B330に対して本来の着信者アドレスを開示したくない場合があるからである。例えば、発信者B300がインターネット上の通信販売業者などである場合には、本来の着信者アドレスをむやみに開示してしまうとメーリングリストなどを通じてこの着信者アドレスが他の業者に拡散し、着信者B230が不要なダイレクトメールなどを着信せねばならない事態が生じ得るからである

。なお、このアドホックアドレスには、着信者B230にメールを配達すべきか否かを示すコンテキスト情報と本来の着信者アドレスが埋め込まれているので、コンテキスト情報に含まれる配達条件を満たす場合にのみ本来の着信者アドレスを用いてメールを配達することができる、言い換えると、たとえアドホックアドレスが他の業者などに伝搬したとしても、コンテキスト情報に含まれる配達条件を満たさない場合には、かかる業者から着信者B230に対するメールを着信者B230に配達しないようにすることができる。

第28図に示した発信者端末B320は、発信者B330がインターネットB400を介したメール授受をおこなう際に利用する端末装置であり、着信者端末B220は、着信者B230がインターネットB400を介したメール授受をおこなう際に利用する端末装置である。これらの発信者端末B320および着信者端末B220は、一般に普及しているパーソナルコンピュータ（PC）であり、WEBブラウザソフトと電子メールソフト（メール）とがインストールされ、ルータRを介して発側IP網B300および着側IP網B200にそれぞれ接続されている。なお、かかる発側IP網B300および着側IP網B200は、それぞれルータRを介してインターネットB400に接続されている。

アドホックアドレス発行サーバB120は、着信者B230の要求に応答してアドホックアドレスを発行するサーバ装置であり、HTTP通信部B121、暗号鍵テーブルB122、ユーザテーブルB123およびアドホックアドレス生成部B124を有する。かかるアドホックアドレス発行サーバB120は、市販の5 PCやワークステーション(WS)にこれらの機能部に対応するプログラムをインストールするとともに各テーブルをハードディスク装置などに格納することにより実現できる。このアドホックアドレス発行サーバB120は、着側IP網B200にファイアウォール(FW)を介して接続されたLANB100に接続されている。なお、このアドホックアドレス発行サーバB120は請求項28の開10 示用アドレス発行装置に対応し、HTTP通信部B121は請求項29の受付手段および開示用アドレス返信手段に対応し、アドホックアドレス生成部B124は請求項29の開示用アドレス生成手段に対応し、暗号鍵テーブルB122は請求項30の暗号鍵テーブルに対応する。

HTTP通信部B121は、HTTP(Hyper Text Transfer Protocol)にしたがった通信をおこなう処理部であり、暗号鍵テーブルB122は、アドホックメールを発行する際に利用する複数の暗号鍵をそれぞれ鍵IDに対応付けて格納したテーブルである。第29図は、かかる暗号鍵テーブルB122の一例を示す図である。同図に示すように、この暗号鍵テーブルB122では、暗号鍵「0x34d2a36b」を鍵ID17に対応付けて格納し、暗号鍵「0xe48ab21f」を鍵ID18に対応付けて格納し、暗号鍵「0xab46fc9a」を鍵ID19に対応付けて格納し、暗号鍵「0xe6a3b13b」を鍵ID19に対応付けて格納している。20

ユーザテーブルB123は、アドホックメールの発行を希望するユーザである着信者B230のアクセスを認証する際に用いられるテーブルであり、それぞれユーザ名とパスワードを対応付けて格納する。第30図は、第28図に示したユーザテーブルB123の一例を示す図である。同図に示すように、このユーザテーブルB123では、ユーザ名「suzuki」にパスワード「ef34szq5s」を対応付けて格納し、ユーザ名「tanaka」にパスワード「ew4902sa」を対応付けて格納し25

、ユーザ名「yamada」にパスワード「wf4wsfa3s」を対応付けて格納している。

アドホックアドレス生成部B 1 2 4は、本発明に係るアドホックアドレスの生成をおこなう処理部であり、図示したように条件コードテーブルB 1 2 4 aを有する。具体的には、このアドホックアドレス生成部B 1 2 4では、着信者アドレスと、コンテキスト情報を形成する条件の種別・組合せを示す条件コード及びこの条件コードに対応するコンテキスト情報とから開示用のアドホックアドレスを生成する。なお、アドホックアドレスの具体的な生成手順については後述するが、このアドホックアドレス生成部B 1 2 4では、暗号鍵テーブルB 1 2 2の暗号鍵を用いた暗号化技術によりアドホックメールに着信者アドレスおよびコンテキスト情報を埋め込む。

このアドホックアドレス生成部B 1 2 4に内在した条件コードテーブルB 1 2 4 aは、上記コンテキスト情報を形成する配送条件の種別・組合せを示す条件コードを格納したテーブルである。第31図は、この条件コードテーブルB 1 2 4 aの一例を示す図である。同図に示すように、この条件コードテーブルB 1 2 4 aには、配送条件の組合せパターンと組合せコードとが対応づけて格納される。

図中のパターン「S」は、発信者アドレスを配送条件としてコンテキスト情報を含ませることを意味し、このパターンの組合せコードは「0000」である。パターン「D」は、発信者アドレスのドメイン名（発ドメイン）を配送条件としてコンテキスト情報を含ませることを意味し、このパターンの組合せコードは「0001」である。パターン「E」は、アドホックアドレスの有効期限を配送条件としてコンテキスト情報を含ませることを意味し、このパターンの組合せコードは「0010」である。パターン「F」は、アドホックアドレスの着信開始日を配送条件としてコンテキスト情報を含ませることを意味し、このパターンの組合せコードは「0011」である。パターン「S E」は、上記パターンSの発信者アドレスとパターンEの有効期限を配送条件としてコンテキスト情報を含ませることを意味し、このパターンの組合せコードは「0100」である。パターン「D E」は、上記パターンDの発ドメインとパターンEの有効期限を配送条件としてコンテキスト情報を

含ませることを意味し、このパターンの組合せコードは「0101」である。パターン「D F」は、上記パターンDの発ドメインとパターンFの着信開始日を配送条件としてコンテキスト情報を含ませることを意味し、このパターンの組合せコードは「0110」である。パターン「D E F」は、上記パターンDの発ドメイン、パターンEの有効期限およびパターンFの着信開始日を配送条件としてコンテキスト情報を含ませることを意味し、このパターンの組合せコードは「0111」である

これらの組合せパターンのいずれかに対応する組合せコードをアドホックアドレスに埋め込むことにより、アドホックアドレスにどのようなコンテキスト情報が埋め込まれているかを把握することができる。なお、ここでは発信者アドレス、発ドメイン、有効期限および着信開始日をコンテキスト情報を形成する配送条件とする場合を示したが、本発明はこれに限定されるものではなく、これら以外の配送条件を対象とすることもできる。この場合には、配送条件に対応する組合せコードを条件コードテーブルB 1 2 4 aに登録すれば良い。

次に、第28図に示したアドホックメール転送サーバB 1 1 0の構成について説明する。第28図に示したアドホックメール転送サーバB 1 1 0は、アドホックメールを受け付けた際に、このアドホックメールから着信者アドレスの復元およびコンテキスト情報の抽出をおこない、抽出したコンテキスト情報に含まれる配送条件を満たす場合に、復元した着信者アドレスにアドホックメールを配達するサーバ装置である。

このアドホックメール転送サーバB 1 1 0は、アドホックアドレス発行サーバB 1 2 0と同様に市販のP Cやワークステーション(WS)にこれらの機能部に対応するプログラムをインストールするとともに復号鍵テーブルB 1 1 2をハードディスク装置などに格納することにより実現できる。このアドホックアドレス転送サーバB 1 1 0は、着側I P網B 2 0 0にファイアウォール(FW)を介して接続されたL A N B 1 0 0に接続されており、メール通信部B 1 1 1と、復号鍵テーブルB 1 1 2と、フィルタ処理部B 1 1 3と、転送処理部B 1 1 4とから

なる。なお、このアドホックメール転送サーバB 1 1 0は請求項28のメール転送装置に対応し、フィルタ処理部B 1 1 3は請求項29のフィルタ処理手段に対応し、転送処理部B 1 1 4は請求項29の転送処理手段に対応し、復号鍵テーブルB 1 1 2は請求項30の復号鍵テーブルに対応する。

5 メール通信部B 1 1 1は、SMT P標準に基づき他のメールサーバとメールを送着信する処理部であり、復号鍵テーブルB 1 1 2は、共通鍵暗号系の場合にはアドホックアドレス発行サーバB 1 2 0が有する第29図に示した暗号鍵テーブルB 1 2 2と同一のものである。なお、公開鍵暗号系の場合には、たとえば周知のR S A暗号の秘密鍵と公開鍵のペアを生成しておき、その公開鍵を暗号鍵テーブルB 1 2 2に登録するとともに、秘密鍵を復号鍵テーブルB 1 1 2に登録することになる。

10 フィルタ処理部B 1 1 3は、他のメールサーバからアドホックメールの配達要求（中継要求）を受け付け、受け付けたアドホックメールの宛先をなすアドホックアドレスに含まれるコンテキスト情報（配達条件）に基づいて当該アドホックメールを本来の着信者アドレスに配達すべきか否かを判定する処理部である。すなわち、このフィルタ処理部B 1 1 3は、配達条件を満たすアドホックメールのみを配達対象とし、それ以外を配達外とする一種のフィルタリング処理をおこなうことになる。

15 具体的には、このフィルタ処理部B 1 1 3では、復号鍵テーブルB 1 1 2に格納された復号鍵を用いてアドホックアドレスを復号化処理して、着信者アドレスおよびコンテキスト情報を取得し、取得したコンテキスト情報に含まれる配達条件を用いて当該アドホックメールを配達対象とすべきか否かを判定する。なお、配達条件を満たしており配達対象とすべきと判定した場合には、アドホックアドレスから取り出した着信者アドレスとアドホックメールを転送処理部B 1 1 4に受け渡して転送依頼をおこなう。

20 転送処理部B 1 1 4は、フィルタ処理部B 1 1 3によって配達対象であると判定されたアドホックメールを本来の着信者アドレスに転送する処理をおこなう処

理部であり、この着信者アドレスはフィルタ処理部B113がアドホックアドレスから復号したものを利用する。

次に、第28図に示したアドホックアドレス発行サーバB120によるアドホックアドレスの発行手順について説明する。第33図は、第28図に示したアドホックアドレス発行サーバB120によるアドホックアドレスの発行手順を示すシーケンス図である。なお、ここではアドホックアドレスの発行をHTTP通信により実現するものとし、アドホックアドレス発行サーバB120のURLは、あらかじめ利用者B230に通知しておくものとする。

同図に示すように、着信者B230が、着信者端末B220上のWEBブラウザにアドホックアドレス発行サーバB120のURLを入力して該アドホックアドレス発行サーバB120に対してアクセス要求をおこなうと（ステップS110）、このアドホックアドレス発行サーバB120は、着信者端末B220に対してユーザ認証ページを返送する（ステップS120）。第33図は、ユーザ認証ページの一例を示す図である。同図に示すように、このユーザ認証ページB500には、ユーザ名とパスワードを入力する入力枠が設けられている。

ここで、着信者B230がユーザ認証ページB500上でユーザ名およびパスワードを入力してアドホックアドレス発行サーバB120に対して認証要求をおこなうと（ステップS130）、このアドホックアドレス発行サーバB120がユーザ認証をおこなう（ステップS140）。具体的には、受信したユーザ名およびパスワードに対応する組み合わせが、第30図で示したユーザテーブルB123に登録されているか否かを確認する。

そして、ユーザが正当であると認証された場合には、アドホックアドレス発行サーバB120は着信者端末B230に対してアドホックアドレス発行ページを送信する（ステップS150）。第34図は、アドホックアドレス発行ページの一例を示す図である。同図に示すように、このアドホックアドレス発行ページB600は、着信者アドレスと配送条件を入力する入力枠が設けられており、具体的には、発信者指定の有無、有効期限の有無、着信開始時指定の有無を選択す

る入力枠と、ありの場合の指定アドレス（ドメイン名）、有効期限、着信開始日を指定する入力枠とがそれぞれ設けられている。

ここで、着信者B230がアドホックアドレス発行ページB600上で着信者アドレスと配送条件を入力して送信をおこなうと、着信者アドレスRと配送条件（コンテキスト情報）Cとを指定したアドホックアドレス要求がアドホックアドレス発行サーバB120に対しておこなわれる（ステップSB160）。

アドホックアドレス発行サーバB120が、このアドホックアドレス要求を受け付けたならば、着信者アドレスRと配送条件（コンテキスト情報）Cを用いたアドホックアドレス生成処理がおこなわれ（ステップSB170）、生成されたアドホックアドレスTが着信者端末B220に通知される（ステップSB180）。着信者B230が、かかるアドホックアドレスTを入手したならば、このアドホックアドレスTを発信者B320に対して通知する（ステップSB190）。なお、このアドホックアドレスTの通知は、電話、メール、FAXなどいかなる情報伝達手段を用いても構わない。

次に、第32図のステップSB170に示したアドホックアドレス生成処理手順についてさらに具体的に説明する。第35図は、第32図のステップSB170に示したアドホックアドレス生成処理手順を示すフローチャートであり、第36図は、アドホックアドレス生成の具体例を示す図である。なお、ここでは説明の便宜上、着信者アドレスRが「tanaka@mail.isp-A.ne.jp」であり、配送条件Cが指定発信者アドレス「suzuki@mail.isp-B.ne.jp」と指定有効期限「2003年8月31日」であるものとする。また、第36図中の「B」は2進データ（バイナリーデータ）を示し、「H」は16進データ（ヘキサデータ）を示している。なお、後述する第41図でも同様の表記を用いる。

第35図に示すように、アドホックアドレス生成部B124は、着信者アドレスのユーザ名部分を圧縮符号化する（ステップSB201）。具体的には、第36図に示すように、着信者アドレスRのユーザ名部分をハフマン符号化などにより圧縮符号化してバイナリーデータB22. p 「0000 0100 1010 0111 0100 001

0 0100 01」を取得した後、2バイト以上のバイト単位のデータとなるようにビット0を追加し、16進データ（Hexデータ）B 2 2. p 「04b74244」を取得する。

その後、暗号鍵テーブルB 1 2 2を参照して、暗号鍵と当該鍵の鍵IDとを取得する（ステップSB 2 0 2）。ここでは、第9図に示したように、鍵ID\_k = 18、K=e48ab21fであるものとする。

その後、コンテキスト情報を符号化する（ステップSB 2 0 3）。具体的には、第36図に示すように、指定発信者アドレス「suzuki@mail.isp-B.ne.jp」のハッシュ値を用いて符号化して16進データB 2 1 2. S = 「4d52」を取得するとともに、指定有効期限「2003年8月31日」を符号化してB 2 1 2. E = 「053a」を取得し、これらをつなげてB 2 1 1 = 「4d52053a」を取得する。そして、このデータに配送条件の組み合わせを符号化した16進データ（コンテキスト符号化データ）B 2 1 1 = 「04」を取得し、これらのデータをつなげて16進データB 2 1 = 「044d52053a」を取得する。

さらに具体的に説明すると、配送条件に指定発信者アドレスを含む場合には、指定発信者アドレスのハッシュ値の下位16ビットを符号化情報とし、配送条件に発ドメインが含まれる場合には、指定発ドメインの単語数を4ビット整数符号化し、これに指定発ドメインのハッシュ値の下位12ビットを付加して符号化情報とすることができます。また、配送条件に有効期限や着信開始日が含まれる場合には、2000年1月1日から当該指定日までの日数を16ビット整数符号化することができる。なお、「Nビット整数符号化」とは、0から（2のN乗-1）までの整数値をNビットの二進数で表現することを意味し、たとえば「7」を3ビット整数符号化すると「111」となり、5ビット整数符号化すると「00111」となる。

その後、着信者アドレス符号化データとコンテキスト符号化データを連結する（ステップSB 2 0 4）。具体的には、第36図に示したように、着信者アドレス符号化データB 2 2. p とコンテキスト符号化データB 2 1とを連結して16

進データB2p=「044d52053a04b74244」を生成し、データB2pが16バイト未満の場合に乱数をパディングして、16進データB2pp=「044d52053a04b742444436e21a2a6b3f56」を取得する。なお、パディング処理に乱数を用いる理由は、既知平文攻撃による暗号鍵解析を困難にするためである。

5 その後、連結したデータを暗号鍵を用いて暗号化し（ステップSB205）、この暗号化データに暗号鍵IDを連結した後（ステップSB206）、ドメイン名を追加する（ステップSB207）。具体的には、16進データB2ppを暗号鍵Kで暗号化して暗号データB2を取得し、この暗号データB2の後に識別子ID\_kを7ビット整数符号化したデータB1をつなげて135ビットのデータを生成し、このデータをBASE32で符号化（テキスト化）し27文字の文字列に変換し、この文字列の後に「@adhoc.isp-A.ne.jp」というドメイン名を追加する。

10

15 上記一連の処理をおこなうことにより、着信者アドレス「tanaka@mail.isp-A.ne.jp」と、指定発信者アドレス「suzuki@mail.isp-B.ne.jp」および指定有効期限「2003年8月31日」からなる配送条件（コンテキスト情報）に基づいて、「bk2crrop15ab3z26b21csq69bai@adhoc.isp-A.ne.jp」というアドホックアドレスを生成できることになる。

20 次に、第28図に示したアドホックメール転送サーバB110によるアドホックメールの転送手順について説明する。第37図は、第28図に示したアドホックメール転送サーバB110によるアドホックメールの転送手順を示すシーケンス図である。

25 同図に示すように、発信者330が発信者端末320を用いてアドホックアドレスTを宛先とするメールの発信操作をおこなうと（ステップSB301）、このメールが発側メールサーバB310にメール送信される（ステップSB302）。そして、この発側メールサーバB310は、メール転送サーバとしての通常動作により宛先アドレスのドメイン名に対応するメールサーバへメール送信要求をおこなう（ステップSB303）。ここで、このアドホックアドレスのドメイ

ン名がアドホックメール転送サーバB 110のホスト名となっているので、このメール送信要求はアドホックメール転送サーバB 110に受信される。

そして、このアドホックメール転送サーバB 110は、メール転送要求の宛先であるアドホックアドレスTに基づいて後述するフィルタ処理をおこない（ステップSB 304）、当該メール送信要求を受け付けるか棄却するかを判定する。

そして、このフィルタ処理によりメール転送要求を受け付けると判定した場合には、宛先をなすアドホックアドレスTに基づいて着信者アドレスRを取得し、発側メールサーバB 310に対してメール送信許可をおこなう（ステップSB 305）。

このメール送信許可を受け付けた発側メールサーバB 310は、アドホックメールをアドホックメール転送サーバB 110にデータ転送し（ステップSB 306）、アドホックメール転送サーバB 110は、アドホックメールの宛先をなすアドホックアドレスから復元した着信者アドレスのドメイン名を確認して転送先を判断し（ステップSB 307）、このドメイン名が示す着側メールサーバB 210に当該アドホックメールを転送する（ステップSB 308）。

着信者端末B 220は、着信者B 230の到着メール確認操作を契機としてメール確認要求を着側メールサーバB 220に送信し（ステップSB 309）、このメール確認要求に応答して着側メールサーバB 220は、アドホックメールを着信者端末B 220に送信する（ステップSB 310）。

なお、上記ステップSB 304のフィルタ処理によりメール転送要求を受け付ける（棄却する）と判定した場合には、発側メールサーバB 310に対してメール受信拒否メッセージを送信してメール転送をおこなわないこととなる。

次に、第37図のステップSB 304で示したフィルタ処理について具体的に説明する。第38図は、第37図のステップSB 304で示したフィルタ処理手順を示すフローチャートである。同図に示すように、アドホックアドレス転送サーバB 110のフィルタ処理部B 113は、まず最初に宛先アドレスのユーザ名部分から暗号鍵IDと暗号データを抽出する（ステップSB 401）。具体的に

は、第36図に示したアドホックアドレスの生成手順と概ね逆順で復号化処理がおこなわれ、アドホックアドレスのユーザ名部分から「bk2crrop15ab3z26b21csq69bai」から7ビットの暗号鍵ID「0010010」と復号対象となる暗号データが取り出される。

5 その後、暗号鍵IDに対応する復号鍵を復号鍵テーブル112から取得し（ステップS402）、取得した復号鍵を用いて暗号データを復号する（ステップS403）。具体的には、共通鍵暗号系の場合には、第36図に示したように鍵ID=18に対応する16進データの復号鍵「e48ab21f」を取得し、この復号鍵を用いて暗号データを復号化することにより、16進データB2pp=「044d5205  
10 3a04b742444436e21a2a6b3f56」を取得する。

その後、復号データから着信者アドレス符号化データとコンテキスト符号化データを取り出し（ステップSB404）、コンテキスト符号化データからコンテキスト情報を抽出して転送可否を判定する（ステップSB405）。具体的には、16進データB2ppから着信者アドレス符号化データB22..pとコンテキスト符号化データB21を抽出するとともに、コンテキスト符号化データB21から指定発信者アドレスのハッシュ値B212..Sと有効期限B212..Eを配  
15 送条件として抽出して、この配達条件を満たしているか否かにより転送可否を判定することになる。

具体的には、アドホックメールの発信者アドレスのハッシュ値を求めて符号化し、このハッシュ値がアドホックメールから抽出したハッシュ値B212..Sと一致する場合には、正当な発信者からのメールであると判定する。また、現在の年月日が有効期限B212..Eを超過しているか否かによって正当なメールであるか否かを判定する。すなわち、正当な発信者からのメールであり、かつ、有効期限内のメールである場合には、転送可能であると判定することになる。

25 そして、転送不可と判断した場合には（ステップSB406否定）、メールを破棄し（ステップSB407）、転送可と判定した場合には（ステップSB406肯定）、着信者アドレス符号化データから着信者アドレスのユーザ名部分を復

元し（ステップSB408）、これにドメイン名を付加した着信者アドレスにメールを転送する（ステップSB409）。

上述してきたように、本実施例5では、着信者B230に配達するメールの配達条件を示す配達条件情報（コンテキスト情報）と着信者アドレスに基づいて開示用のアドホックアドレスを発行するアドホックアドレス発行サーバB120と、かかるアドホックアドレスを宛先とするメールを着信した際に、該アドホックアドレスから着信者アドレスの復元およびコンテキスト情報の抽出をおこない、該抽出したコンテキスト情報に含まれる配達条件を当該メールが満たす場合に、該メールの宛先をアドホックアドレスから復元した着信者アドレスに置き換えて当該メールを転送するアドホックメール転送サーバB130とを設けるよう構成したので、メールアドレスの漏洩および拡散に伴う該メールアドレスの用途外使用を抑制することができる。特に、本来の着信者アドレスのみならずアドホックアドレスが漏洩した場合であっても、本来の用途に使用されたアドホックアドレスのみを着信者に配達することが可能となる。

15 (実施例6)

ところで、上記実施例5では、着信者アドレスRを単に圧縮符号化したデータを暗号化することとしたが、この着信者アドレスRは固定的なものであるので第三者の差分攻撃による暗号鍵解析に対して脆弱である。そこで、この実施例6では、差分攻撃による暗号鍵解析に強い実施例を示すこととする。

20 第39図は、本実施例6に係るメール配達システムのシステム構成を示す図である。同図に示すものは、第28図に示すシステムと比べてアドホックアドレス発行サーバB120およびアドホックメール転送サーバB110にそれぞれ乱数列テーブルB125およびB115が設けられている点が異なる。なお、この乱数列テーブルB125は、請求項11の乱数列テーブルに対応する。

25 乱数列テーブルB125は、アドホックアドレス発行サーバB120がアドホックアドレスを生成する際に、着信者アドレスRを乱数でスクランブル（可逆変換処理）するために利用するテーブルである。すなわち、アドホックアドレス生

成部B124は、乱数列テーブルB125から乱数列を取り出したならば、着信者アドレスRと乱数列の排他的論理和（EXOR）をとって着信者アドレスRをその都度スクランブルする。乱数列との排他的論理和をとっているので、かかる処理は周知のバーナム暗号と呼ばれる乱数式換字暗号をおこなっていることになる。  
·5 第40図は、乱数列テーブルB125の一例を示す図である。同図に示すように、この乱数列テーブルB125は、16ビットからなる複数の乱数列にそれぞれインデックスを付与したテーブルである。

乱数列テーブルB115は、アドホックメール転送サーバB110がアドホックアドレスから着信者アドレスRを可逆変換により取得する際に利用するテーブルであり、上記乱数列テーブルB125と同一のものである。バーナム暗号化された着信者アドレスRの暗号データに再度同じ乱数列をEXORすると、乱数列がキャンセルされ着信者アドレスRを復元することができる。

次に、これらの乱数列テーブルB125およびB115からの乱数列の選択について説明する。これらの乱数列テーブルB125およびB115は、第40図に示したようにインデックスを対応付けて付与しているので、基本的には、インデックスを授受すれば使用する乱数列を特定することができる。しかしながら、アドホックメール以外に別途乱数列のインデックスを受け渡すことは効率的ではない。このため、本実施例6では、アドホックアドレスの生成に用いられる情報の一部に基づき乱数列テーブルB125およびB115から抽出する乱数を決定することとしている。具体的には、乱数列テーブルB125およびB115の乱数の数をNとし、各乱数に対して0～N-1のインデックス番号を割り当てておき、配送条件データB21のハッシュ値をNで割った剩余値をインデックス番号とする乱数を乱数列テーブルB125およびB115から選択している。

次に、第39図に示したアドホックアドレス生成部B124によるアドホックアドレス生成の具体例について説明する。第41図は、第39図に示したアドホックアドレス生成部B124によるアドホックアドレス生成の具体例を示す図である。同図に示すものは、実施例5で説明した第36図の具体例に対応するもので

ある。なお、あらかじめ乱数列テーブルB 1 2 5およびB 1 1 5の乱数の数をNとし、各乱数に対して0～N-1のインデックス番号を割り当てておく。

第4 1図に示すように、ここでは第3 6図に示した具体例と同様にして、まず着信者アドレスRのユーザ名部分を圧縮符号化してバイナリーデータB 2 2. p  
5 「0000 0100 1010 0111 0100 0010 0100 01」を取得した後、2バイト以上のバ  
イト単位のデータとなるようにビット0を追加し、16進データB 2 2. p 「04  
b74244」を取得する。

その後、配送条件Cから得られる16進データB 2 1=「044d52053a」のハッシュ値をNで割った剰余値をキーとして乱数列テーブルB 1 2 5を検索し、この  
10 キーをインデックス番号として持つ乱数列のバイナリーデータB 2 2. r=「00  
11011010101011」を取得し、取得した乱数列B 2 2. rと16進データB 2 2.  
p 「04b74244」との排他的論理和演算をおこなって、データB 2 2を生成する。  
なお、これ以降の処理は、第3 6図に示したものと同様である。

上述してきたように、本実施例6では、アドホックアドレス発行サーバB 1 2  
15 0とアドホックメール転送サーバB 1 1 0にそれぞれ乱数列テーブルB 1 2 5お  
よびB 1 1 5を設け、配送条件から得られるデータを用いて乱数列テーブルB 1  
2 5から乱数列を選択するよう構成したので、第三者の差分攻撃による暗号鍵解  
析を困難にすることができる。

#### (実施例7)

ところで、上記実施例5および6では、着信者アドレス自体を圧縮符号化してアドホックアドレスに埋め込む場合を示したが、本発明はこれに限定されるものではなく、着信者アドレスに代えてアドレス識別子を用いる場合に適用することもできる。すなわち、本来アドホックメールを利用する意味は、着信者アドレスを発信者に知らせない点にあるため、できる限り着信者アドレスは発信者に秘密にすることが望ましい。また、着信者アドレスは一定長ではなく様々なデータ長のものがあるので、着信者アドレス自体を用いることはアドホックアドレスのデータ長を確定的に一定長にできず効率的ではない。特に、着信者アドレスに様々

なドメイン名が混在する場合には、上記実施例5および6を拡張してドメイン名を含む着信者アドレス全体を埋め込み対象とする必要があるが、着信者アドレス全体を埋め込み対象とすると、ますますアドホックアドレスのデータ長が長くなる。このため、本実施例7では、着信者アドレスRに代えてアドホックメールア  
5 ドレス識別子を用いる場合を示すこととする。

第42図は、本実施例7に係るメール配達システムのシステム構成を示す図である。同図に示すものは、第28図および第39図に示すシステムと比べてアドホックアドレス発行サーバB120およびアドホックメール転送サーバB110にそれぞれアドレステーブルB126およびB116が設けられている点が異なる。  
10 なお、かかるアドレステーブルB126およびB116は、請求項14のアドレステーブルに対応する。

アドレステーブルB126は、アドホックアドレス発行サーバB120がアドホックアドレスを生成する際に、着信者アドレスRをアドホックメールアドレス識別子に置き換えるために利用するテーブルである。第43図は、第42図に示したアドレステーブルB126の一例を示す図である。同図に示すように、このアドレステーブルB126は、アドホックメールアドレス識別子と着信者アドレスとを対応付けて記憶したテーブルであり、ここでは着信者アドレス「tanap@oc  
15 e.com」にアドホックメールアドレス識別子「TN」を対応付け、着信者アドレス「suzup@pla.com」にアドホックメールアドレス識別子「SZ」を対応付けた場合  
アドレステーブルB116は、アドホックメール転送サーバB110の転送処理部B114が、アドホックアドレスから抽出したアドホックメールアドレス識別子に対応する着信者アドレスRを特定する際に利用するテーブルであり、上記アドレステーブルB126と同一のものである。  
20

そして、アドホックアドレス発行サーバB120のアドホックアドレス生成部B124は、実施例5および6のように着信者アドレスの圧縮符号化をおこなうのではなく、アドレステーブルB126を用いて着信者アドレスをアドホックメ  
25

ールアドレス識別子に置き換える処理をおこなうことになる。

また、アドホックメール転送サーバB 1 1 0では、フィルタ処理部B 1 1 3による配送条件の判定の結果、転送すべきものと判定したもののみについて、アドホックメールアドレス識別子に対応する着信者アドレスをアドレステーブルB 1 5 1 6から抽出することになる。つまり、アドホックメールアドレス識別子から着信者アドレスへの変換は、アドホックメールが転送すべきと判定された場合にのみおこなわれる所以、かかるアドレス変換に伴う処理負荷は大きくない。

上述してきたように、本実施例7では、アドホックアドレス発行サーバB 1 2 0およびアドホックメール転送サーバB 1 1 0にそれぞれアドレステーブルB 1 10 2 6およびB 1 1 6を設けておき、着信者アドレスの変わりにアドホックメールアドレス識別子を用いるよう構成したので、（1）着信者アドレスの漏洩をより一層防止することができ、（2）アドホックアドレスのデータ長を確定的に一定長にできるという効果を奏する。特に、ドメイン名の異なる各種メールアドレスを対象とする場合に効率的なものとなる。

15 なお、上記実施例5～7では、暗号鍵テーブルB 1 2 2やユーザテーブルB 1 2 3、乱数列テーブルB 1 2 5およびアドレステーブルB 1 2 6などをアドホックアドレス発行サーバB 1 2 0内に設ける場合を示したが、これらの各種テーブルをサーバ外部に配設することもできる。また、上記実施例5～7では、暗号化および復号化をおこなう際の暗号化ロジック等についての説明を省略したが、ハッシュ値を求めるための一方向性関数としては周知のMD 5、SHA-1などのアルゴリズムを用いることができ、暗号アルゴリズムとしてはDES、RC 5、FEA Lなどの共通鍵暗号アルゴリズムやRSAなどの公開鍵暗号アルゴリズムを用いることができる。さらに、上記実施例5～7では、暗号鍵テーブルB 1 2 2からの暗号鍵の選択についての説明を省略したが、ランダムな選択、同一発行25 先についてラウンドロビンで選択するなどの選択をおこなえば良い。

また、上記実施例5～7では、配送条件としてアドホックアドレスへの通信の利用を許可する発信者アドレス、アドホックアドレスへの通信の利用を許可する

発ドメイン、アドホックアドレスの有効期限またはアドホックアドレスの有効開始日若しくはこれらの組み合わせを用いた場合を示したが、本発明はこれに限定されるものではなく、メールのデータ量の上限を示すデータサイズや、メールのサブジェクトフィールドの先頭から所定の文字数分の文字列が示すサブジェクトワードなどを配送条件に含めることもできる。この場合には、これらの指定の種別・組み合わせに関する情報を条件コードテーブルB 1 2 4 a およびB 1 1 3 a に登録すれば良い。

なお、上記実施例5～7では、メール配送システムを機能面から説明することとしたが、実際には、アドホックアドレス発行サーバB 1 2 0 やアドホックメール転送サーバB 1 1 0 は、市販のコンピュータにより実現することができるので、これらのコンピュータにそれぞれプログラムをインストールすれば良いことになる。このプログラムは、ハードディスク装置等の二次記録媒体やROMからCPUにロードする場合だけではなく、CD-Rなどの記録メディアからロードしても良い。たとえば、CD-Rからプログラムをロードする場合には、あらかじめアドホックアドレス発行サーバB 1 2 0 用プログラムおよびアドホックメール転送サーバB 1 1 0 用プログラムなどをCD-R（装置ごと別個のCD-Rであっても良い）に格納しておき、このCD-Rを各装置のCD-R読取装置に装着してプログラムをロードすることになる。

以上説明したように、本発明によれば、受信者に通信する際の通信条件を示す通信条件情報および受信者識別子に基づいて開示用識別子を生成しておき、生成した開示用識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立するよう構成したので、受信者識別子ではなく開示用識別子を開示することになり、もって受信者識別子の漏洩に伴う該受信者識別子の用途外利用を防止することができる。特に、かかる開示用識別子が第三

者に漏洩した場合であっても、第三者の通信端末からの通信要求に無条件に応答して該通信端末と受信者通信端末の通信を確立するのではなく、通信条件を満たす場合にのみこの間の通信を確立することとしたので、開示用識別子の用途外利用についても抑制することが可能となる。

5 また、本発明によれば、受信者通信端末に配送するメールの配送条件を示す配送条件情報および受信者を一意に特定する受信者アドレスに基づいて開示用アドレスを生成しておき、生成した開示用アドレスを宛先アドレスとするメールを受け付けた場合に、該メールの宛先アドレスである開示用アドレスから受信者アドレスおよび配送条件情報を復元し、復元した配送条件情報に包摂される配送条件を満たす場合に、メールを受信者通信端末に対して配送するよう構成したので、受信者アドレスではなく開示用アドレスを開示することになり、もって受信者アドレスの漏洩に伴う該受信者アドレスの用途外利用を防止することができる。特に、かかる開示用アドレスが第三者に漏洩した場合であっても、第三者によるメールを無条件に受信者通信端末に配送するのではなく、配送条件を満たす場合にのみこのメールを配送することとしたので、開示用アドレスの用途外利用についても抑制することが可能となる。

また、本発明によれば、受信者電話端末に通話接続する際の通話条件情報および受信者電話番号に基づいて開示用電話番号を生成しておき、生成した開示用電話番号に基づく通話接続要求を受け付けた場合に、該通話接続要求に含まれる開示用電話番号から受信者電話番号および通話条件情報を復元し、復元した通話条件情報に含まれる通話条件を満たす場合に、発信者電話端末と受信者電話端末とを通話接続するよう構成したので、受信者電話番号ではなく開示用電話番号を開示することになり、もって受信者電話番号の漏洩に伴う該受信者電話番号の用途外利用を防止することができる。特に、かかる開示用電話番号が第三者に漏洩した場合であっても、第三者による開示用電話番号を用いた通話要求に応答して無条件に受信者電話端末に通話接続するのではなく、通話条件を満たす場合にのみ通話接続することとしたので、開示用電話番号の用途外利用についても抑制する

ことが可能となる。

また、本発明によれば、受信者通信端末において通信条件情報および受信者識別子に基づいて開示用識別子を生成するよう構成したので、受信者識別子を他の装置に開示する必要がなくなり、効率良く受信者識別子の拡散を防止することができる。  
5

また、本発明によれば、受信者通信端末と通信可能な所定の仲介装置において通信条件情報および受信者識別子に基づいて開示用識別子を生成するよう構成したので、各受信者通信端末に新たな装置やプログラムを装備しなくとも、開示用識別子を利用することができる。

10 また、本発明によれば、受信者通信端末と送信者通信端末の間に介在する中継システムが、復元された受信者識別子および／または通信条件情報を受信者通信端末に通知するよう構成したので、受信者通信端末自身で通信要求を受け付けるか否かを判断することができる。

また、本発明によれば、受信者通信端末と送信者通信端末の間に介在する中継  
15 システムが、復元された通信条件情報に含まれる通信条件を満たさない場合の処理内容を決定するよう構成したので、システム全体として通信条件を満たない場合の一貫した対応を取ることができる。

また、本発明によれば、受信者通信端末が、復元された通信条件情報に含まれる通信条件を満たさない場合の処理内容を決定するよう構成したので、各受信者  
20 が自ら処理内容を自由に決定することができる。

また、本発明によれば、通信条件情報が、開示用識別子を開示する発信者を限定する発信者限定情報を含み、少なくとも通信要求をおこなった発信者が前記発信者限定情報に含まれる限定条件と一致すると判断した場合に、この通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立するよう構成したので  
25 、たとえば発ドメイン名などを正当な開示先として指定されているような場合に、この発ドメイン名を有する発信者からの通信要求のみを受け付けることが可能になる。

また、本発明によれば、通信条件情報に開示用識別子を開示する開示先を特定する開示先特定情報を含ませるよう構成したので、開示用識別子が不正に用途外利用された場合に、この開示用識別子が本来誰に開示したものであるかを調べることができる。

5 また、本発明によれば、復元された通信条件情報に含まれる通信条件を満たさない場合に、通信要求を拒絶するよう構成したので、通信条件を満たさない通信要求を受信者にとってトランスペアレント（透過的）な位置づけにすることができる。

また、本発明によれば、復元した通信条件情報に含まれる通信条件を満たさない場合に、通信要求にかかわらず受信者通信端末と異なる所定の通信端末と発信者通信端末との通信を確立するよう構成したので、開示識別子が用途外利用されている状況を所定の通信端末で把握することができる。

また、本発明によれば、各受信者の受信者識別子および該受信者の受信者通信端末に通信する際の通信条件を示す通信条件情報を仲介装置に登録しておき、発信者通信端末から開示用識別子の開示要求を受け付けた場合に、この仲介装置に登録された受信者識別子および通信条件情報に基づいて開示用識別子を生成するよう構成したので、開示用識別子を作成する度に受信者識別子を受け渡す必要をなくし、もってより一層受信者識別子を保護することができる。

また、本発明によれば、開示用識別子の開示要求をおこなう発信者が開示要求をおこなう資格を有するか否かを判定し、発信者が資格を有さないと判定された場合に通信要求を棄却するよう構成したので、発信者の資格のない者からの開示要求を棄却し、もって開示用識別子の漏洩を防止することができる。

また、本発明によれば、受信者通信端末に通信する際の仮の通信条件を示す仮通信条件情報および受信者識別子に基づいて仮開示用識別子を生成し、生成した仮開示用識別子を仲介装置に登録しておき、発信者通信端末から開示用識別子の開示要求を受け付けた場合に、この仲介装置に登録された仮開示用識別子および通信条件情報を開示用識別子書換装置に送信して開示用識別子の書き換えを要求

し、この要求に応答して仮開示用識別子および通信条件情報をから開示用識別子を生成するよう構成したので、仲介装置に受信者識別子を開示しなくとも開示用識別子を用いた通信確立をおこなうことができる。

また、本発明によれば、仲介装置が書換要求をおこなう資格を有するか否かを5 仮開示用識別子に基づいて判定し、当該仲介装置が資格を有さないと判定された場合に書換要求を棄却するよう構成したので、書換をおこなう資格のない仲介装置からの要求を廃棄することができる。

また、本発明によれば、受信者識別子および通信条件情報を所定の公開鍵で暗号化して開示用識別子を生成し、生成した開示用識別子に基づく通信を受け付け10 場合に、該開示用識別子を公開鍵に対応する秘密鍵で復号化して受信者識別子および通信条件情報を復元するよう構成したので、周知の公開鍵暗号系を用いて通信条件情報を開示用識別子に埋め込むことができる。

また、本発明によれば、所定の共通する鍵を用いて受信者識別子および通信条件情報を暗号化して開示用識別子を生成し、生成した開示用識別子に基づく通信を受け付けた場合に、該開示用識別子を当該共通する鍵で復号化して受信者識別子および通信条件情報を復元するよう構成したので、共通する鍵を利用するあら15 ゆる暗号化手法を用いて通信条件情報を開示用識別子に埋め込むことができる。

また、本発明によれば、受信者識別子および通信条件情報を所定の共通鍵で暗号化して開示用識別子を生成し、生成した開示用識別子に基づく通信を受け付け20 場合に、該開示用識別子を共通鍵で復号化して受信者識別子および通信条件情報を復元するよう構成したので、周知の共通鍵暗号系を用いて通信条件情報を開示用識別子に埋め込むことができる。

また、本発明によれば、通信条件情報をおよび受信者識別子に基づいて開示用識別子を生成する際に、通信条件情報を第三者による改竄ができない形式で開示用25 識別子に含めるよう構成したので、通信条件情報の書き替えなどの不正行為を防止することができる。

また、本発明によれば、通信条件情報が通信条件の種別または組み合わせを

含み、復元に際してはこの開示用識別子から通信条件の種別または組み合わせを抽出し、抽出した通信条件の種別および組み合わせにしたがって該開示用識別子から受信者識別子および通信条件情報を復元するよう構成したので、同じシステム内で様々な通信条件を使い分けることができる。

5 また、本発明によれば、開示用識別子付与装置が、受信者通信端末に通信する際の通信条件を示す通信条件情報および受信者識別子に基づいて開示用識別子を生成するとともに、生成した開示用識別子を発信者通信端末に通知し、中継システムは、開示用識別子付与装置により付与された開示用識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立するよう構成したので、受信者識別子ではなく開示用識別子を開示することになり、もって受信者識別子の漏洩に伴う該受信者識別子の用途外利用を防止することができる。特に、かかる開示用識別子が第三者に漏洩した場合であっても、第三者の通信端末からの通信要求に無条件に応答して該通信端末と受信者通信端末の通信を確立するのではなく、通信条件を満たす場合にのみこの間の通信を確立することとしたので、開示用識別子の用途外利用についても抑制することが可能となる。

20 また、本発明によれば、開示用識別子付与装置が受信者通信端末の一部をなすよう構成したので、受信者識別子を他の装置に開示する必要がなくなり、効率良く受信者識別子の拡散を防止することができる。

25 また、本発明によれば、開示用識別子付与装置が受信者通信端末および中継システムのいずれとも異なる仲介装置とするよう構成したので、各受信者通信端末に新たな装置やプログラムを装備しなくとも、開示用識別子を利用することができる。

また、本発明によれば、受信者通信端末に通信する際の通信条件を示す通信条件情報および受信者識別子に基づいて生成された開示用識別子に基づく発信者通

信端末からの通信要求を受け付けた場合に、該開示用識別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立するよう構成したので、受信者識別子ではなく開示用識別子を開示することになり  
5 、もって受信者識別子の漏洩に伴う該受信者識別子の用途外利用を防止することができる。特に、かかる開示用識別子が第三者に漏洩した場合であっても、第三者の通信端末からの通信要求に無条件に応答して該通信端末と受信者通信端末の通信を確立するのではなく、通信条件を満たす場合にのみこの間の通信を確立することとしたので、開示用識別子の用途外利用についても抑制することが可能となる。  
10

また、本発明によれば、受信者に通信する際の通信条件を示す通信条件情報および受信者識別子に基づいて開示用識別子を生成しておき、生成した開示用識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立するよう構成したので、受信者識別子ではなく開示用識別子を開示することになり、もって受信者識別子の漏洩に伴う該受信者識別子の用途外利用を防止することができる。特に、かかる開示用識別子が第三者に漏洩した場合であっても、第三者の通信端末からの通信要求に無条件に応答して該通信端末と受信者通信端末の通信を確立するのではなく、通信条件を満たす場合にのみこの間の通信を確立することとしたので、開示用識別子の用途外利用についても抑制することが可能となる。  
15  
20

また、本発明によれば、受信者通信端末に通信する際の通信条件を示す通信条件情報および受信者識別子に基づいて生成された開示用識別子に基づく発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から受信者識別子および通信条件情報を復元し、復元した通信条件情報に含まれる通信条件を満たす場合に、通信要求にしたがって発信者通信端末と受信者通信端末の通信を確立す  
25

るよう構成したので、受信者識別子ではなく開示用識別子を開示することになり、もって受信者識別子の漏洩に伴う該受信者識別子の用途外利用を防止することができる。特に、かかる開示用識別子が第三者に漏洩した場合であっても、第三者の通信端末からの通信要求に無条件に応答して該通信端末と受信者通信端末の通信を確立するのではなく、通信条件を満たす場合にのみこの間の通信を確立することとしたので、開示用識別子の用途外利用についても抑制することが可能となる。

また、本発明によれば、開示用アドレス発行装置が、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスに基づいて開示用アドレスを発行し、メール転送装置が、開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから着信者アドレスの復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を当該メールが満たす場合に、該メールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するよう構成したので、メールアドレスの漏洩および拡散に伴う該メールアドレスの用途外使用を抑制することができる。特に、本来の着信者アドレスを第三者に開示する必要がなくなるため、本来のメールアドレス自体の漏洩および拡散を防ぐことができるとともに、たとえ開示用アドレスが漏洩した場合であっても、本来の正しい使用がなされたもの以外は着信者に配送されないため、不正な開示用アドレスの無効化を図ることができる。

また、本発明によれば、開示用アドレス発行装置が、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスを受け付け、受け付けた配送条件情報と着信者アドレスを暗号化して開示用アドレスを生成し、生成した開示用アドレスを着信者通信端末に返信し、メール転送装置は、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、抽出したメールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するよう構成したので、

暗号化技術を用いて開示用アドレスの生成並びに開示用アドレスからの着信者アドレスの復元および配送条件情報の抽出をおこなうことができるため、周知の暗号技術を用いて通信条件情報を開示用アドレスに埋め込み等が可能になるとともに、併せて第三者による通信条件情報の改竄を防止することができる。

5 また、本発明によれば、暗号鍵テーブルに登録した所定の暗号鍵を用いて配送条件情報と着信者アドレスを暗号化して開示用アドレスを生成し、暗号鍵テーブルに登録された各暗号鍵に対応する復号鍵を登録した復号鍵テーブルから復号鍵を取り出し、取り出した復号鍵を用いて開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこなうよう構成したので、様々な暗号鍵を場合によって使い分かつ暗号強度を高めることができる。

10 また、本発明によれば、暗号鍵テーブルに登録した所定の暗号鍵を用いて暗号化する暗号化対象データのデータ長が所定長未満である場合に該所定長を満たすように乱数を付加するよう構成したので、第三者による既知平文攻撃による暗号鍵解析を困難にすることができる。

15 また、本発明によれば、複数の暗号鍵にそれぞれ鍵識別子を対応付けて暗号鍵テーブルに登録し、配送条件情報と着信者アドレスを暗号化する際に用いた暗号鍵の鍵識別子を開示用アドレスに含め、開示用アドレスから抽出した鍵識別子を有する復号鍵を復号鍵テーブルから取り出し、取り出した復号鍵を用いて開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこなうよう構成したので、開示用アドレスを媒介として鍵識別子を受け渡し、もって効率的な鍵配送をおこなうことができる。

20 また、本発明によれば、暗号鍵テーブルと復号鍵テーブルは、複数の共通鍵にそれぞれ鍵識別子を対応付けて登録した同一のテーブルとするよう構成したので、テーブルの同期さえ確保すれば周知の共通鍵暗号系を用いて効率良く暗号化処理・復号化処理をおこなうことができる。

25 また、本発明によれば、複数の公開鍵をそれぞれ鍵識別子と対応付けて暗号鍵テーブルに登録し、この暗号鍵テーブルに登録された各公開鍵に対応する秘密鍵

をそれぞれ同じ鍵識別子に対応づけて復号鍵テーブルに登録するよう構成したので、周知の公開鍵暗号系を利用して効率良く暗号化処理・復号化処理をおこなうことができる。

また、本発明によれば、開示用アドレスへの通信の利用を許可する発信者アドレス、開示用アドレスへの通信の利用を許可する発ドメイン、開示用アドレスの有効期限または開示用アドレスの有効開始日若しくはこれらの組み合わせを配送条件情報とするよう構成したので、開示用アドレスの利用者、利用者群、利用可能期間を特定してかかる利用者または利用者群若しくは期間に適合しないメールを配送対象外とし、もって着信者がダイレクトメールなどを大量に受信せねばならない状況を回避することができる。

また、本発明によれば、指定された配送条件の種別・組み合わせを開示用アドレスに含めるよう構成したので、アドレスの開示先ごとに最適な配送条件・種別の組み合わせを選択することが可能となり、より適切な条件の設定が可能となる。また、開示用アドレスにすべての配送条件に対応する欄を設ける必要がなくなり、開示用アドレスのデータ長を短くすることができる。

また、本発明によれば、発信者アドレスまたは発ドメインを配送条件情報とする場合に、該発信者アドレスまたは発ドメインのハッシュ値の全部または一部を開示用アドレスに含めるよう構成したので、配送条件情報のデータ長を一定にし、もって開示用アドレスのデータ長を制限することができる。

また、本発明によれば、複数の乱数列を記憶する乱数列テーブルから抽出した乱数列を用いて暗号化対象となる情報の一部を可逆変換処理するよう構成したので、第三者の差分攻撃による暗号鍵解析を困難にすることができる。

また、本発明によれば、開示用アドレスの生成に用いられる情報の一部に基づき乱数列テーブルから抽出する乱数を決定するよう構成したので、乱数列の選択を開示用アドレスの生成に用いられる情報の一部に依存させ、もって乱数列の選択を容易かつ効率的なものにすることができる。

また、本発明によれば、配送条件情報に基づいて乱数列テーブルから乱数列を

選択し、選択した乱数列を用いて着信者アドレスを可逆変換処理するよう構成したので、上記差分攻撃による暗号鍵解析の困難化のほかに、本来最も漏洩を防ぐべき着信者アドレスをスクランブルし、もって第三者への着信者アドレスの漏洩を防ぐことができる。

5 また、本発明によれば、開示用アドレス発行装置およびメール転送装置に対して、各着信者アドレスを所定のアドレス識別子に対応付けて記憶するアドレステーブルを設け、着信者アドレスに対応するアドレステーブルに記憶したアドレス識別子と配送条件情報を暗号化して開示用アドレスを生成し、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化してアドレス識別子の復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、開示用アドレスから復元したアドレス識別子に対応する前記アドレステーブルに記憶した着信者アドレスにメールの宛先を置き換えて当該メールを転送するよう構成したので、開示用アドレスのデータ長を一定にするとともに、アドレステーブル上のアドレス識別子を  
10 秘密にすることにより第三者の既知平文攻撃による暗号鍵解析を困難にすること  
ができる。

また、本発明によれば、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスに基づいて開示用アドレスを発行し、開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから着信者アドレスの復元および配送条件情報の抽出をおこない、抽出した配送条件情報に含まれる配送条件を当該メールが満たす場合に、該メールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するよう構成したので、メールアドレスの漏洩および拡散に伴う該メールアドレスの用途外使用を抑制することができる。特に、本来の着信者アドレスを第三者に開示する必要がなくなるため、本来のメールアドレス自体の漏洩および拡散を防ぐことができるとともに、たとえ開示用アドレスが漏洩した場合であっても、本来の正しい使用がなされたもの以外は着信者に配送されないため、不正な開示用アドレスの無効化を図ることがで  
20  
25

きる。

また、本発明によれば、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスを受け付け、受け付けた配送条件情報と着信者アドレスを暗号化して開示用アドレスを生成し、生成した開示用アドレスを着信者通信端末に返信するとともに、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、抽出したメールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するよう構成したので、暗号化技術を用いて開示用アドレスの生成並びに開示用アドレスからの着信者アドレスの復元および配送条件情報の抽出をおこなうことができるため、周知の暗号技術を用いて通信条件情報を開示用アドレスに埋め込み等が可能になるとともに、併せて第三者による通信条件情報の改竄を防止することができる。

また、本発明によれば、暗号鍵テーブルに登録した所定の鍵識別子を有する暗号鍵を用いて受け付けた配送条件情報と着信者アドレスを暗号化して開示用アドレスを生成し、所定の鍵識別子を有する復号鍵を復号鍵テーブルから取り出し、取り出した復号鍵を用いて開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこなうよう構成したので、様々な暗号鍵を場合によって使い分けつつ暗号強度を高めることができる。

また、本発明によれば、開示用アドレスの利用を許可する発信者アドレス、開示用アドレスの利用を許可する発ドメイン、開示用アドレスの有効期限または開示用アドレスの有効開始日若しくはこれらの組み合わせを配送条件情報とするよう構成したので、開示用アドレスの利用者、利用者群、利用可能期間を特定してかかる利用者または利用者群若しくは期間に適合しないメールを配送対象外とし、もって着信者がダイレクトメールなどを大量に受信せねばならない状況を回避することができる。

また、本発明によれば、指定された配送条件の種別・組み合わせを開示用アド

レスに含めるよう構成したので、アドレスの開示先ごとに最適な配送条件・種別の組み合わせを選択することが可能となり、より適切な条件の設定が可能となる。また、開示用アドレスにすべての配送条件に対応する欄を設ける必要がなくなり、開示用アドレスのデータ長を短くすることができる。

5 また、本発明によれば、各着信者アドレスを所定のアドレス識別子に対応付けてアドレステーブルに記憶しておき、着信者アドレスに対応するアドレステーブルに記憶したアドレス識別子と配送条件情報を暗号化して開示用アドレスを生成するとともに、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化してアドレス識別子の復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、開示用アドレスから復元したアドレス識別子に対応するアドレステーブルに記憶した着信者アドレスにメールの宛先を置き換えて当該メールを転送するよう構成したので、開示用アドレスのデータ長を一定にできるとともに、アドレステーブル上のアドレス識別子を秘密にすることにより第三者の既知平文攻撃による暗号鍵解析を困難にできる。

また、本発明によれば、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスに基づいて開示用アドレスを発行するとともに、開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから着信者アドレスの復元および配送条件情報の抽出をおこない、抽出した配送条件情報に含まれる配送条件を当該メールが満たす場合に、該メールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するよう構成したので、メールアドレスの漏洩および拡散に伴う該メールアドレスの用途外使用を抑制することができる。特に、本来の着信者アドレスを第三者に開示する必要がなくなるため、本来のメールアドレス自体の漏洩および拡散を防ぐことができるとともに、たとえ開示用アドレスが漏洩した場合であっても、本来の正しい使用がなされたもの以外は着信者に配送されないため、不正な開示用アドレスの無効化を図ることができる。

また、本発明によれば、着信者に配送するメールの配送条件を示す配送条件情報と着信者アドレスを受け付け、受け付けた配送条件情報と記着信者アドレスを暗号化して開示用アドレスを生成し、生成した開示用アドレスを着信者通信端末に返信するとともに、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、抽出したメールの宛先を開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するよう構成したので、暗号化技術を用いて開示用アドレスの生成並びに開示用アドレスからの着信者アドレスの復元および配送条件情報の抽出をおこなうことができるため、周知の暗号技術を用いて通信条件情報を開示用アドレスに埋め込み等が可能になるとともに、併せて第三者による通信条件情報の改竄を防止することができる。

また、本発明によれば、暗号鍵テーブルに登録した所定の鍵識別子を有する暗号鍵を用いて配送条件情報と着信者アドレスを暗号化して開示用アドレスを生成するとともに、所定の鍵識別子を有する復号鍵を復号鍵テーブルから取り出し、取り出した復号鍵を用いて開示用アドレスを復号化して着信者アドレスの復元および配送条件情報の抽出をおこなうよう構成したので、様々な暗号鍵を場合によって使い分けつつ暗号強度を高めることができる。

また、本発明によれば、開示用アドレスの利用を許可する発信者アドレス、開示用アドレスの利用を許可する発ドメイン、開示用アドレスの有効期限または前記開示用アドレスの有効開始日若しくはこれらの組み合わせを配送条件情報とするよう構成したので、開示用アドレスの利用者、利用者群、利用可能期間を特定してかかる利用者または利用者群若しくは期間に適合しないメールを配送対象外とし、もって着信者がダイレクトメールなどを大量に受信せねばならない状況を回避することができる。

また、本発明によれば、指定された配送条件の種別・組み合わせを開示用アドレスに含めるよう構成したので、アドレスの開示先ごとに最適な配送条件・種別

の組み合わせを選択することが可能となり、より適切な条件の設定が可能となる。また、開示用アドレスにすべての配送条件に対応する欄を設ける必要がなくなり、開示用アドレスのデータ長を短くすることができる。

また、本発明によれば、各着信者アドレスを所定のアドレス識別子に対応付けてアドレステーブルに記憶しておく、着信者アドレスに対応するアドレステーブルに記憶したアドレス識別子と配送条件情報を暗号化して開示用アドレスを生成するとともに、開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化してアドレス識別子の復元および配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、開示用アドレスから復元したアドレス識別子に対応するアドレステーブルに記憶した着信者アドレスにメールの宛先を置き換えて当該メールを転送するよう構成したので、開示用アドレスのデータ長を一定にするとともに、アドレステーブル上のアドレス識別子を秘密にすることにより第三者の既知平文攻撃による暗号鍵解析を困難にすることができます。

15

#### 産業上の利用可能性

以上のように、本発明に係る通信方法、通信システム、中継システム、通信プログラムおよび中継システム用プログラムは、受信者を一意に特定する受信者識別子を用いた発信者通信端末からの通信要求に応答して該発信者通信端末と受信者通信端末との通信をおこなう通信方法、通信システム、中継システム、通信プログラム、中継システム用プログラム、メール配送システム、メール配送方法およびメール配送プログラムに有用であり、特に、受信者識別子が当該受信者の想定外の用途に利用されることを防ぐことができる通信方法、通信システム、中継システム、通信プログラム、中継システム用プログラム、メール配送システム、メール配送方法およびメール配送プログラムに適している。

## 請求の範囲

1. 受信者を一意に特定する受信者識別子を用いた発信者通信端末からの通信

5 要求に応答して該発信者通信端末と受信者通信端末との通信をおこなう通信方法

であつて、

前記受信者に通信する際の通信条件を示す通信条件情報および前記受信者識別子に基づいて開示用識別子を生成する開示用識別子生成工程と、

前記開示用識別子生成工程により生成された開示用識別子に基づく前記発信者

10 通信端末からの通信要求を受け付けた場合に、該開示用識別子から前記受信者識

別子および前記通信条件情報を復元する復元工程と、

前記復元工程により復元された通信条件情報に含まれる通信条件を満たす場合

に、前記通信要求にしたがって前記発信者通信端末と前記受信者通信端末の通信

を確立する通信確立工程と

15 を含んだことを特徴とする通信方法。

2. 前記開示用識別子生成工程は、受信者通信端末に配達するメールの配達条

件を示す配達条件情報および前記受信者を一意に特定する受信者アドレスに基づ

いて開示用アドレスを生成し、前記復元工程は、前記開示用識別子生成工程によ

20 り生成された開示用アドレスを宛先アドレスとするメールを受け付けた場合に、

該メールの宛先アドレスである開示用アドレスから前記受信者アドレスおよび前

記配達条件情報を復元し、前記通信確立工程は、前記復元工程により復元された

配達条件情報に包摂される配達条件を満たす場合に、前記メールを前記受信者通

信端末に対して配達することを特徴とする請求の範囲第1項に記載の通信方法。

25

3. 前記開示用識別子生成工程は、前記受信者電話端末に通話接続する際の通

話条件情報および受信者電話番号に基づいて開示用電話番号を生成し、前記復元

工程は、前記開示用識別子生成工程により生成された開示用電話番号に基づく通話接続要求を受け付けた場合に、該通話接続要求に含まれる開示用電話番号から前記受信者電話番号および前記通話条件情報を復元し、前記通信確立工程は、前記復元工程により復元された通話条件情報を含まれる通話条件を満たす場合に、  
5 前記発信者電話端末と前記受信者電話端末とを通話接続することを特徴とする請求の範囲第1項に記載の通信方法。

4. 前記開示用識別子生成工程は、前記受信者通信端末において前記通信条件情報および前記受信者識別子に基づいて前記開示用識別子を生成することを特徴  
10 とする請求の範囲第1項、第2項または第3項に記載の通信方法。

5. 前記開示用識別子生成工程は、前記受信者通信端末と通信可能な所定の仲介装置において前記通信条件情報および前記受信者識別子に基づいて前記開示用識別子を生成することを特徴とする請求の範囲第1項、第2項または第3項に記  
15 載の通信方法。

6. 前記受信者通信端末と前記送信者通信端末の間に介在する中継システムが  
、前記復元工程により復元された前記受信者識別子および／または前記通信条件  
情報を前記受信者通信端末に通知する通知工程をさらに含んだことを特徴とする  
20 請求の範囲第1項～第5項のいずれか一つに記載の通信方法。

7. 前記受信者通信端末と前記送信者通信端末の間に介在する中継システムが  
、前記復元工程により復元された前記通信条件情報に含まれる通信条件を満たさ  
ない場合の処理内容を決定する第1の決定工程をさらに含んだことを特徴とする  
25 請求の範囲第1項～第6項のいずれか一つに記載の通信方法。

8. 前記受信者通信端末が、前記復元工程により復元された前記通信条件情報

に含まれる通信条件を満たさない場合の処理内容を決定する第2の決定工程をさらに含んだことを特徴とする請求の範囲第1項～第6項のいずれか一つに記載の通信方法。

5 9. 前記通信条件情報は、前記開示用識別子生成工程により生成された開示用識別子を開示する発信者を限定する発信者限定情報を含み、前記通信確立工程は、少なくとも前記通信要求をおこなった発信者が前記発信者限定情報に含まれる限定条件と一致すると判断した場合に、前記通信要求にしたがって前記発信者通信端末と前記受信者通信端末の通信を確立することを特徴とする請求の範囲第1項～第8項のいずれか一つに記載の通信方法。

10 10. 前記通信条件情報は、前記開示用識別子生成工程により生成された開示用識別子を開示する開示先を特定する開示先特定情報を含んだことを特徴とする請求の範囲第1項～第8項のいずれか一つに記載の通信方法。

15 11. 前記通信確立工程は、前記復元工程により復元された通信条件情報に含まれる通信条件を満たさない場合に、前記通信要求を拒絶することを特徴とする請求の範囲第1項～第10項のいずれか一つに記載の通信方法。

20 12. 前記通信確立工程は、前記復元工程により復元された通信条件情報に含まれる通信条件を満たさない場合に、前記通信要求にかかわらず前記受信者通信端末と異なる所定の通信端末と発信者通信端末との通信を確立することを特徴とする請求の範囲第1項～第10項のいずれか一つに記載の通信方法。

25 13. 各受信者の受信者識別子および該受信者の受信者通信端末に通信する際の通信条件を示す通信条件情報を前記仲介装置に登録する登録工程をさらに含み、前記開示用識別子生成工程は、発信者通信端末から開示用識別子の開示要求を

受け付けた場合に、前記仲介装置に登録された受信者識別子および前記通信条件情報に基づいて前記開示用識別子を生成することを特徴とする請求の範囲第5項に記載の通信方法。

5 14. 前記開示用識別子の開示要求をおこなう発信者が開示要求をおこなう資格を有するか否かを判定し、前記発信者が資格を有さないと判定された場合に前記通信要求を棄却する棄却工程をさらに含んだことを特徴とする請求の範囲第13項に記載の通信方法。

10 15. 前記受信者通信端末に通信する際の仮の通信条件を示す仮通信条件情報および前記受信者識別子に基づいて仮開示用識別子を生成する仮開示用識別子生成工程と、

前記仮開示用識別子生成工程により生成された仮開示用識別子を前記仲介装置に登録する仮登録工程とをさらに含み、

15 前記開示用識別子生成工程は、  
発信者通信端末から開示用識別子の開示要求を受け付けた場合に、前記仲介装置に登録された仮開示用識別子および前記通信条件情報を開示用識別子書換装置に送信して開示用識別子の書き換えを要求する書換要求工程と、

前記書換要求工程による要求に応答して前記仮開示用識別子および前記通信条件情報から前記開示用識別子を生成する生成工程と  
20 を含んだことを特徴とする請求の範囲第5項に記載の通信方法。

16. 前記仲介装置が書換要求をおこなう資格を有するか否かを前記仮開示用識別子に基づいて判定し、当該仲介装置が資格を有さないと判定された場合に前記書換要求を棄却する棄却工程をさらに含んだことを特徴とする請求の範囲第15項に記載の通信方法。

17. 前記開示用識別子生成工程は、前記受信者識別子および前記通信条件情報をおもに所定の公開鍵で暗号化して前記開示用識別子を生成し、前記復元工程は、前記開示用識別子生成工程により生成された開示用識別子に基づく通信を受け付けた場合に、該開示用識別子を前記公開鍵に対応する秘密鍵で復号化して前記受信者識別子および前記通信条件情報を復元することを特徴とする請求の範囲第1項  
5 ～第16項のいずれか一つに記載の通信方法。

18. 前記開示用識別子生成工程は、所定の共通する鍵を用いて前記受信者識別子および前記通信条件情報を暗号化して前記開示用識別子を生成し、前記復元工程は、前記開示用識別子生成工程により生成された開示用識別子に基づく通信を受け付けた場合に、該開示用識別子を前記共通する鍵で復号化して前記受信者識別子および前記通信条件情報を復元することを特徴とする請求の範囲第1項～  
10 第16項のいずれか一つに記載の通信方法。

19. 前記開示用識別子生成工程は、前記受信者識別子および前記通信条件情報を所定の共通鍵で暗号化して前記開示用識別子を生成し、前記復元工程は、前記開示用識別子生成工程により生成された開示用識別子に基づく通信を受け付けた場合に、該開示用識別子を前記共通鍵で復号化して前記受信者識別子および前記通信条件情報を復元することを特徴とする請求の範囲第1項～第16項のいずれか一つに記載の通信方法。  
15  
20

20. 前記開示用識別子生成工程は、前記通信条件情報を前記受信者識別子に基づいて開示用識別子を生成する際に、前記通信条件情報を第三者による改竄ができない形式で前記開示用識別子に含めることを特徴とする請求の範囲第1項～第19項のいずれか一つに記載の通信方法。  
25

21. 前記通信条件情報は、前記通信条件の種別または組み合わせを含み、前

記復元工程は、前記開示用識別子生成工程により生成された開示用識別子から通信条件の種別または組み合わせを抽出し、抽出した通信条件の種別および組み合わせにしたがって該開示用識別子から前記受信者識別子および前記通信条件情報復元することを特徴とする請求の範囲第1項～第20項のいずれか一つに記載の通信方法。  
5

22. 受信者が利用する受信者通信端末と、該受信者通信端末への通信要求をおこなう発信者通信端末とを中継システムを介して接続し、前記受信者を一意に特定する受信者識別子を用いた発信者通信端末からの通信要求に応答して前記発信者通信端末と受信者通信端末の通信をおこなう通信システムであって、  
10 前記受信者通信端末に通信する際の通信条件を示す通信条件情報および前記受信者識別子に基づいて開示用識別子を生成する開示用識別子生成手段と、前記開示用識別子生成手段により生成された開示用識別子を発信者通信端末に通知する通知手段とを有する開示用識別子付与装置を備え、

15 前記中継システムは、  
前記開示用識別子付与装置により付与された開示用識別子に基づく前記発信者通信端末からの通信要求を受け付けた場合に、該開示用識別子から前記受信者識別子および前記通信条件情報を復元する復元手段と、  
前記復元手段により復元された通信条件情報に含まれる通信条件を満たす場合  
20 に、前記通信要求にしたがって前記発信者通信端末と前記受信者通信端末の通信を確立する通信確立手段と  
を備えたことを特徴とする通信システム。

23. 前記開示用識別子付与装置は、前記受信者通信端末の一部をなすことを特徴とする請求の範囲第22項に記載の通信システム。  
25

24. 前記開示用識別子付与装置は、前記受信者通信端末および前記中継シス

テムのいずれとも異なる仲介装置であることを特徴とする請求の範囲第22項に記載の通信システム。

25. 受信者が利用する受信者通信端末と、該受信者通信端末への通信要求を  
5 おこなう発信者通信端末との間に介在し、前記受信者を一意に特定する受信者識  
別子を用いた発信者通信端末からの通信要求に応答して前記発信者通信端末と受  
信者通信端末との通信を中継する中継システムであって、

前記受信者通信端末に通信する際の通信条件を示す通信条件情報および前記受  
信者識別子に基づいて生成された開示用識別子に基づく前記発信者通信端末から  
10 の通信要求を受け付けた場合に、該開示用識別子から前記受信者識別子および前  
記通信条件情報を復元する復元手段と、

前記復元手段により復元された通信条件情報に含まれる通信条件を満たす場合  
に、前記通信要求にしたがって前記発信者通信端末と前記受信者通信端末の通信  
を確立する通信確立手段と

15 を備えたことを特徴とする中継システム。

26. 受信者を一意に特定する受信者識別子を用いた発信者通信端末からの通  
信要求に応答して該発信者通信端末と受信者通信端末との通信をおこなう通信プ  
ログラムであって、

前記受信者に通信する際の通信条件を示す通信条件情報および前記受信者識別  
子に基づいて開示用識別子を生成する開示用識別子生成手順と、

前記開示用識別子生成手順により生成された開示用識別子に基づく前記発信者  
通信端末からの通信要求を受け付けた場合に、該開示用識別子から前記受信者識  
別子および前記通信条件情報を復元する復元手順と、

25 前記復元手順により復元された通信条件情報に含まれる通信条件を満たす場合  
に、前記通信要求にしたがって前記発信者通信端末と前記受信者通信端末の通信  
を確立する通信確立手順と

をコンピュータに実行させることを特徴とする通信プログラム。

27. 受信者が利用する受信者通信端末と、該受信者通信端末への通信要求をおこなう発信者通信端末との間に介在し、前記受信者を一意に特定する受信者識別子を用いた発信者通信端末からの通信要求に応答して前記発信者通信端末と受信者通信端末との通信を中継する中継システム用プログラムであつて、

前記受信者通信端末に通信する際の通信条件を示す通信条件情報および前記受信者識別子に基づいて生成された開示用識別子に基づく前記発信者通信端末から10の通信要求を受け付けた場合に、該開示用識別子から前記受信者識別子および前記通信条件情報を復元する復元手順と、

前記復元手順により復元された通信条件情報に含まれる通信条件を満たす場合に、前記通信要求にしたがつて前記発信者通信端末と前記受信者通信端末の通信を確立する通信確立手順と

15 をコンピュータに実行させることを特徴とする中継システム用プログラム。

28. 着信者アドレスを有する着信者が利用する着信者通信端末と、前記着信者アドレスを宛先としたメールを発信する発信者通信端末とをネットワークを介して接続し、前記着信者アドレスを宛先としたメールを前記着信者通信端末まで20配送するメール配送システムであつて、

前記着信者に配送するメールの配送条件を示す配送条件情報と前記着信者アドレスに基づいて開示用アドレスを発行する開示用アドレス発行装置と、

前記開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから前記着信者アドレスの復元および前記配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を当該メールが満たす場合に、該メールの宛先を前記開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するメール転送装置と

を備えたことを特徴とするメール配送システム。

29. 前記開示用アドレス発行装置は、

5 前記着信者に配送するメールの配送条件を示す配送条件情報と前記着信者アド  
レスを受け付ける受付手段と、前記受付手段により受け付けた配送条件情報と前  
記着信者アドレスを暗号化して開示用アドレスを生成する開示用アドレス生成手  
段と、前記開示用アドレス生成手段により生成した開示用アドレスを前記着信者  
通信端末に返信する開示用アドレス返信手段とを備え、

前記メール転送装置は、

10 前記開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを  
復号化して前記着信者アドレスの復元および前記配送条件情報の抽出をおこない  
、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出するフィル  
タ処理手段と、前記フィルタ処理手段により抽出されたメールの宛先を前記開示  
用アドレスから復元した着信者アドレスに置き換えて当該メールを転送する転送  
15 処理手段とを備えた

ことを特徴とする請求の範囲第28項に記載のメール配送システム。

30. 前記開示用アドレス発行装置は、複数の暗号鍵を登録した暗号鍵テーブ  
ルをさらに備え、前記開示用アドレス生成手段は、前記暗号鍵テーブルに登録し  
20 た所定の暗号鍵を用いて前記受付手段により受け付けた配送条件情報と前記着信  
者アドレスを暗号化して開示用アドレスを生成し、

前記メール転送装置は、前記暗号鍵テーブルに登録された各暗号鍵に対応する  
復号鍵を登録した復号鍵テーブルをさらに備え、前記フィルタ処理手段は、前記  
所定の暗号鍵に対応する復号鍵を前記復号鍵テーブルから取り出し、取り出した  
25 復号鍵を用いて前記開示用アドレスを復号化して前記着信者アドレスの復元およ  
び前記配送条件情報の抽出をおこなうことを特徴とする請求の範囲第29項に記  
載のメール配送システム。

31. 前記開示用アドレス生成手段は、前記暗号鍵テーブルに登録した所定の暗号鍵を用いて暗号化する暗号化対象データのデータ長が所定長未満である場合に該所定長を満たすように乱数を付加することを特徴とする請求の範囲第30項  
5 に記載のメール配達システム。

32. 前記暗号鍵テーブルは、複数の暗号鍵にそれぞれ鍵識別子を対応付けて登録し、前記開示用アドレス生成手段は、前記配送条件情報と前記着信者アドレスを暗号化する際に用いた暗号鍵の鍵識別子を前記開示用アドレスに含め、前記  
10 フィルタ処理手段は、前記開示用アドレスから抽出した鍵識別子を有する復号鍵を前記復号鍵テーブルから取り出し、取り出した復号鍵を用いて前記開示用アドレスを復号化して前記着信者アドレスの復元および前記配送条件情報の抽出をおこなうことを特徴とする請求の範囲第30項または第31項に記載のメール配達システム。

15

33. 前記暗号鍵テーブルと前記復号鍵テーブルは、複数の共通鍵にそれぞれ鍵識別子を対応付けて登録した同一のテーブルであることを特徴とする請求の範囲第30項、第31項または第32項に記載のメール配達システム。

20

34. 前記暗号鍵テーブルは、複数の公開鍵をそれぞれ鍵識別子と対応付けて登録し、前記復号鍵テーブルは、前記暗号鍵テーブルに登録された各公開鍵に対応する秘密鍵をそれぞれ同じ鍵識別子に対応づけて登録したことを特徴とする請求の範囲第30項、第31項または第32項に記載のメール配達システム。

25

35. 前記開示用アドレス生成手段は、前記開示用アドレスへの通信の利用を許可する発信者アドレス、前記開示用アドレスへの通信の利用を許可する宛名、前記開示用アドレスの有効期限または前記開示用アドレスの有効開始日若

しくはこれらの組み合わせを前記配送条件情報としたことを特徴とする請求の範囲第29項～第34項のいずれか一つに記載のメール配送システム。

36. 前記開示用アドレス生成手段は、指定された配送条件の種別・組み合わせを前記開示用アドレスに含めることを特徴とする請求の範囲第28項～第35項のいずれか一つに記載のメール配送システム。  
5

37. 前記開示用アドレス生成手段は、前記発信者アドレスまたは前記発ドメインを前記配送条件情報とする場合に、該発信者アドレスまたは発ドメインのハッシュ値の全部または一部を前記開示用アドレスに含めることを特徴とする請求の範囲第35項または第36項に記載のメール配送システム。  
10

38. 前記開示用アドレス発行装置は、複数の乱数列を記憶する乱数列テーブルをさらに備え、前記開示用アドレス生成手段は、前記乱数列テーブルから抽出した乱数列を用いて暗号化対象となる情報の一部を可逆変換処理することを特徴とする請求の範囲第29項～第37項のいずれか一つに記載のメール配送システム。  
15

39. 前記開示用アドレス生成手段は、前記開示用アドレスの生成に用いられる情報の一部に基づき前記乱数列テーブルから抽出する乱数を決定することを特徴とする請求の範囲第38項に記載のメール配送システム。  
20

40. 前記開示用アドレス生成手段は、前記配送条件情報に基づいて前記乱数列テーブルから乱数列を選択し、選択した乱数列を用いて前記着信者アドレスを可逆変換処理することを特徴とする請求の範囲第38項または第39項に記載のメール配送システム。  
25

4 1. 前記開示用アドレス発行装置および前記メール転送装置は、各着信者アドレスを所定のアドレス識別子に対応付けて記憶するアドレステーブルをそれぞれさらに備え、前記開示用アドレス生成手段は、前記着信者アドレスに対応する前記アドレステーブルに記憶したアドレス識別子と前記配送条件情報を暗号化して開示用アドレスを生成し、前記フィルタ処理手段は、前記開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して前記アドレス識別子の復元および前記配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、前記転送処理手段は、前記開示用アドレスから復元したアドレス識別子に対応する前記アドレステーブルに記憶した着信者アドレスに前記フィルタ処理手段により抽出されたメールの宛先を置き換えて当該メールを転送することを特徴とする請求の範囲第29項～第40項のいずれか一つに記載のメール配送システム。

4 2. 所定の着信者アドレスを宛先としたメールを該メールを発信した発信者通信端末から前記着信者アドレスを有する着信者が利用する着信者通信端末まで配送するメール配送方法であって、

前記着信者に配送するメールの配送条件を示す配送条件情報と前記着信者アドレスに基づいて開示用アドレスを発行する開示用アドレス発行工程と、

前記開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから前記着信者アドレスの復元および前記配送条件情報の抽出をおこなう復元工程と、

前記復元工程により抽出した配送条件情報に含まれる配送条件を当該メールが満たす場合に、該メールの宛先を前記開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するメール転送工程と

を含んだことを特徴とするメール配送方法。

4 3. 前記開示用アドレス発行工程は、

前記着信者に配送するメールの配送条件を示す配送条件情報と前記着信者アドレスを受け付ける受付工程と、前記受付工程により受け付けた配送条件情報と前記着信者アドレスを暗号化して開示用アドレスを生成する開示用アドレス生成工程と、前記開示用アドレス生成工程により生成した開示用アドレスを前記着信者  
5 通信端末に返信する開示用アドレス返信工程とを含み、

前記メール転送工程は、

前記開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して前記着信者アドレスの復元および前記配送条件情報の抽出をおこない  
、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出するフィル  
10 タ処理工程と、前記フィルタ処理工程により抽出されたメールの宛先を前記開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送する転送  
工程とを含んだ

ことを特徴とする請求の範囲第42項に記載のメール配送方法。

15 4.4. 前記開示用アドレス生成工程は、暗号鍵テーブルに登録した所定の鍵識  
別子を有する暗号鍵を用いて前記受付工程により受け付けた配送条件情報と前記  
着信者アドレスを暗号化して開示用アドレスを生成し、

前記フィルタ処理工程は、前記所定の鍵識別子を有する復号鍵を復号鍵テーブ  
ルから取り出し、取り出した復号鍵を用いて前記開示用アドレスを復号化して前  
20 記着信者アドレスの復元および前記配送条件情報の抽出をおこなうことを特徴と  
する請求の範囲第43項に記載のメール配送方法。

4.5. 前記開示用アドレス生成工程は、前記開示用アドレスの利用を許可する  
発信者アドレス、前記開示用アドレスの利用を許可する発ドメイン、前記開示用  
アドレスの有効期限または前記開示用アドレスの有効開始日若しくはこれらの組  
25 み合わせを前記配送条件情報としたことを特徴とする請求の範囲第43項または  
第44項に記載のメール配送方法。

4.6. 前記開示用アドレス生成工程は、指定された配送条件の種別・組み合わせを前記開示用アドレスに含めることを特徴とする請求の範囲第45項に記載のメール配送方法。

5

4.7. 各着信者アドレスを所定のアドレス識別子に対応付けてアドレステーブルに記憶するアドレス記憶工程をさらに含み、

前記開示用アドレス生成工程は、前記着信者アドレスに対応する前記アドレステーブルに記憶したアドレス識別子と前記配送条件情報を暗号化して開示用アドレスを生成し、前記フィルタ処理工程は、前記開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して前記アドレス識別子の復元および前記配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、前記転送処理工程は、前記開示用アドレスから復元したアドレス識別子に対応する前記アドレステーブルに記憶した着信者アドレスに前記フィルタ処理工程により抽出されたメールの宛先を置き換えて当該メールを転送することを特徴とする請求の範囲第42項～第46項のいずれか一つに記載のメール配送方法。

4.8. 所定の着信者アドレスを宛先としたメールを該メールを発信した発信者通信端末から前記着信者アドレスを有する着信者が利用する着信者通信端末まで配送するメール配送プログラムであって、

前記着信者に配送するメールの配送条件を示す配送条件情報と前記着信者アドレスに基づいて開示用アドレスを発行する開示用アドレス発行手順と、

前記開示用アドレスを宛先とするメールを受け付けた際に、該開示用アドレスから前記着信者アドレスの復元および前記配送条件情報の抽出をおこなう復元手順と、

前記復元手順により抽出した配送条件情報に含まれる配送条件を当該メールが

満たす場合に、該メールの宛先を前記開示用アドレスから復元した着信者アドレスに置き換えて当該メールを転送するメール転送手順と  
をコンピュータに実行させることを特徴とするメール配送プログラム。

5 49. 前記開示用アドレス発行手順は、

前記着信者に配送するメールの配送条件を示す配送条件情報と前記着信者アドレスを受け付ける受付手順と、前記受付手順により受け付けた配送条件情報と前記着信者アドレスを暗号化して開示用アドレスを生成する開示用アドレス生成手順と、前記開示用アドレス生成手順により生成した開示用アドレスを前記着信者  
10 通信端末に返信する開示用アドレス返信手順とを含み、

前記メール転送手順は、

前記開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して前記着信者アドレスの復元および前記配送条件情報の抽出をおこない  
、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出するフィル  
15 タ処理手順と、前記フィルタ処理手順により抽出されたメールの宛先を前記開示  
用アドレスから復元した着信者アドレスに置き換えて当該メールを転送する転送  
処理手順とを含んだ

ことを特徴とする請求の範囲第48項に記載のメール配送プログラム。

20 50. 前記開示用アドレス生成手順は、暗号鍵テーブルに登録した所定の鍵識  
別子を有する暗号鍵を用いて前記受付手順により受け付けた配送条件情報と前記  
着信者アドレスを暗号化して開示用アドレスを生成し、

前記フィルタ処理手順は、前記所定の鍵識別子を有する復号鍵を復号鍵テーブ  
ルから取り出し、取り出した復号鍵を用いて前記開示用アドレスを復号化して前  
記着信者アドレスの復元および前記配送条件情報の抽出をおこなうことを特徴と  
25 する請求の範囲第49項に記載のメール配送プログラム。

51. 前記開示用アドレス生成手順は、前記開示用アドレスの利用を許可する発信者アドレス、前記開示用アドレスの利用を許可する発ドメイン、前記開示用アドレスの有効期限または前記開示用アドレスの有効開始日若しくはこれらの組み合わせを前記配送条件情報としたことを特徴とする請求の範囲第49項または50項に記載のメール配送プログラム。

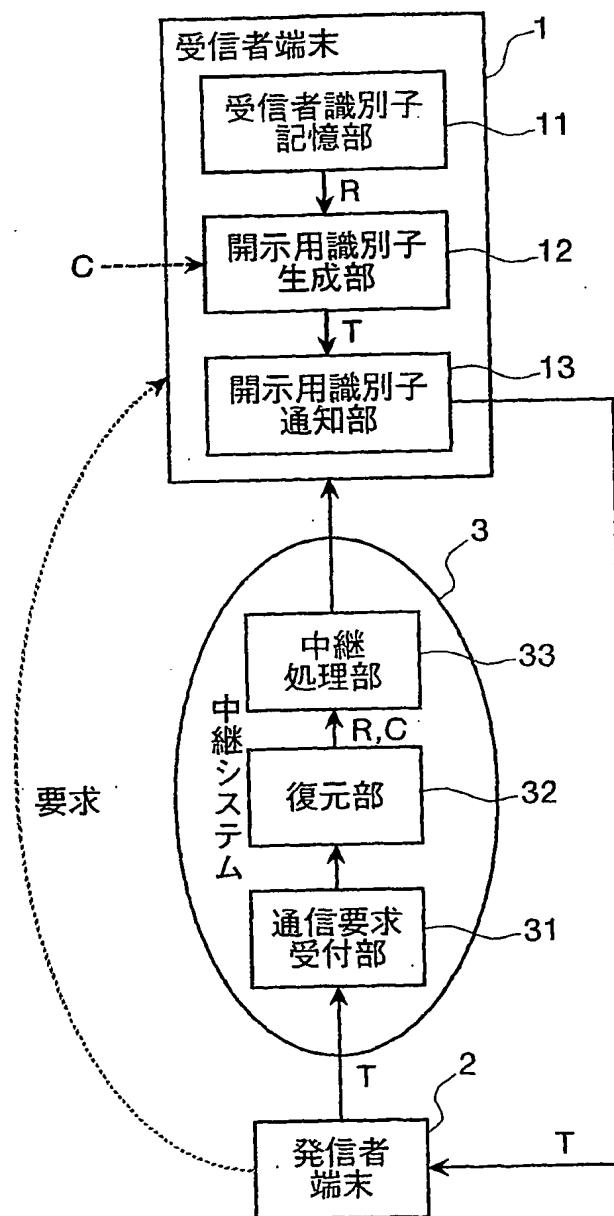
52. 前記開示用アドレス生成手順は、指定された配送条件の種別・組み合わせを前記開示用アドレスに含めることを特徴とする請求の範囲第51項に記載のメール配送プログラム。

10

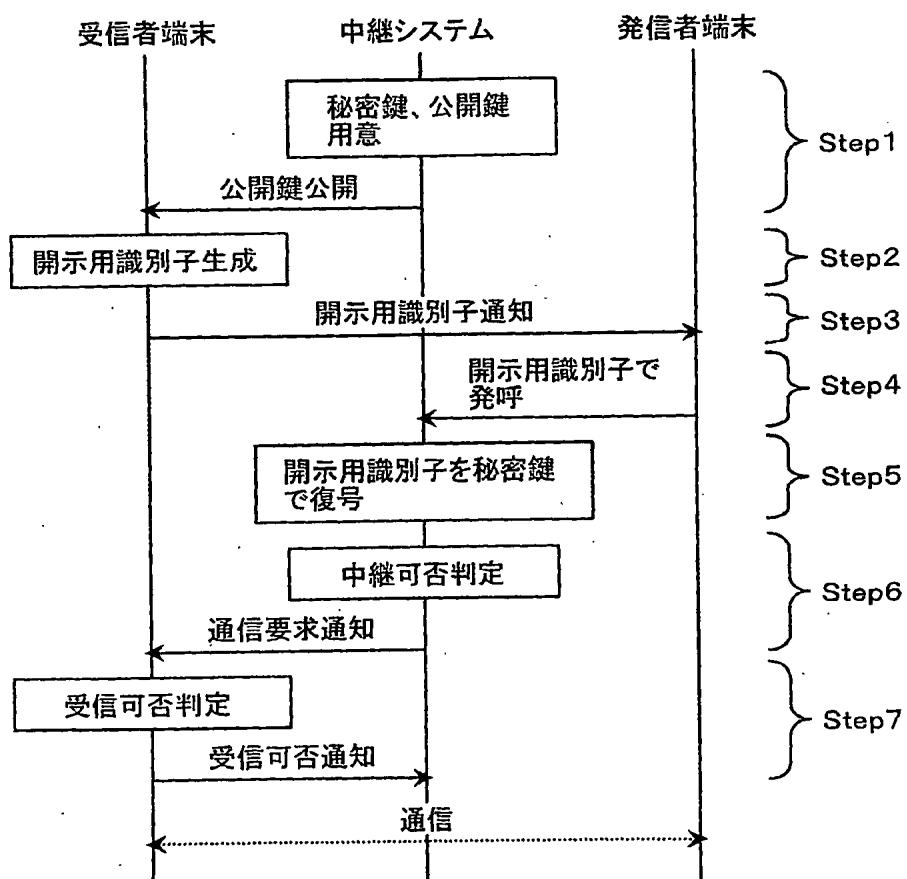
53. 各着信者アドレスを所定のアドレス識別子に対応付けてアドレステーブルに記憶するアドレス記憶手順をさらに含み、

前記開示用アドレス生成手順は、前記着信者アドレスに対応する前記アドレステーブルに記憶したアドレス識別子と前記配送条件情報を暗号化して開示用アドレスを生成し、前記フィルタ処理手順は、前記開示用アドレスを宛先とするメールを着信した際に、該開示用アドレスを復号化して前記アドレス識別子の復元および前記配送条件情報の抽出をおこない、該抽出した配送条件情報に含まれる配送条件を満たすメールを抽出し、前記転送処理手順は、前記開示用アドレスから復元したアドレス識別子に対応する前記アドレステーブルに記憶した着信者アドレスに前記フィルタ処理手順により抽出されたメールの宛先を置き換えて当該メールを転送することを特徴とする請求の範囲第49項～第52項のいずれか一つに記載のメール配送プログラム。

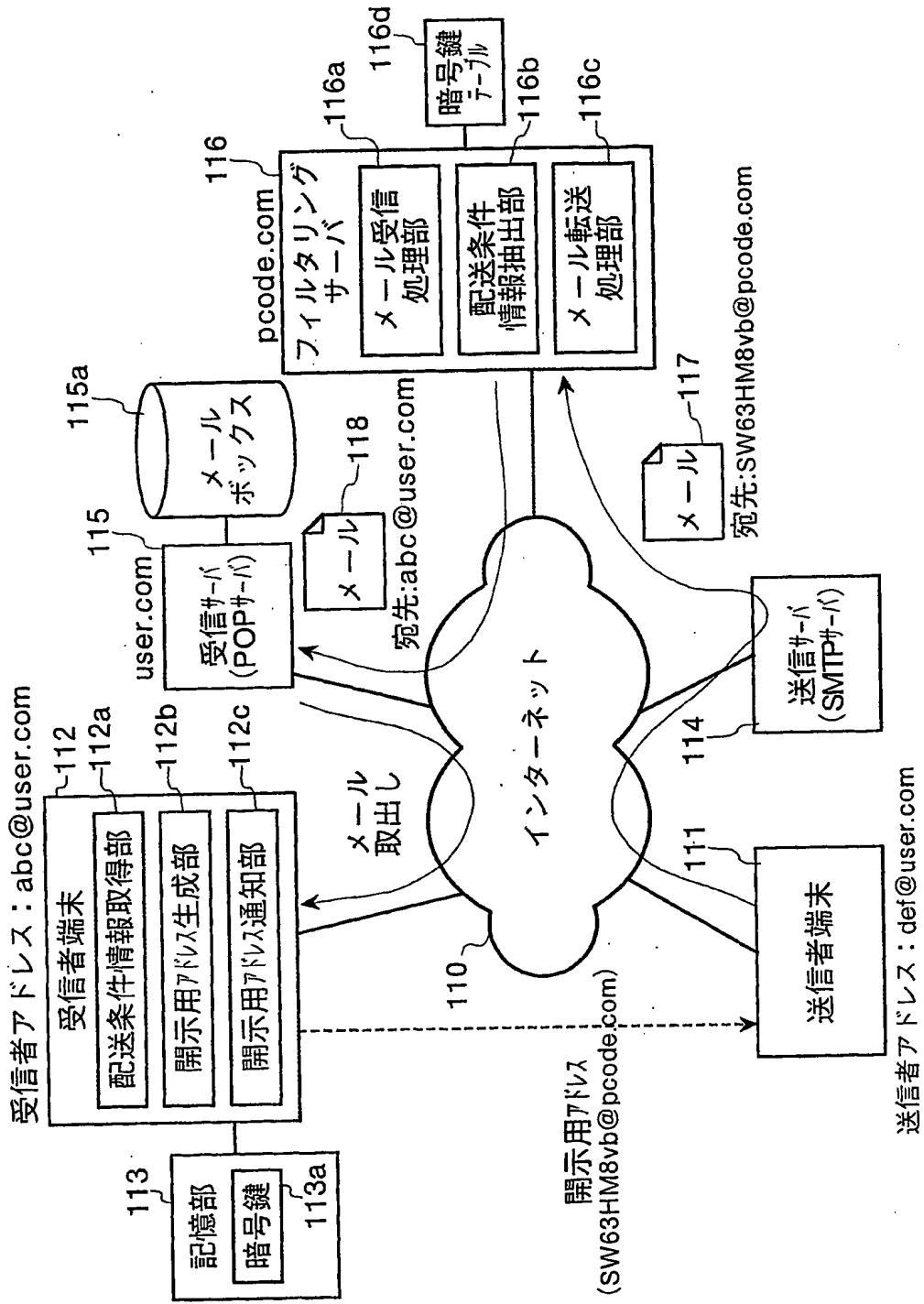
## 第1図



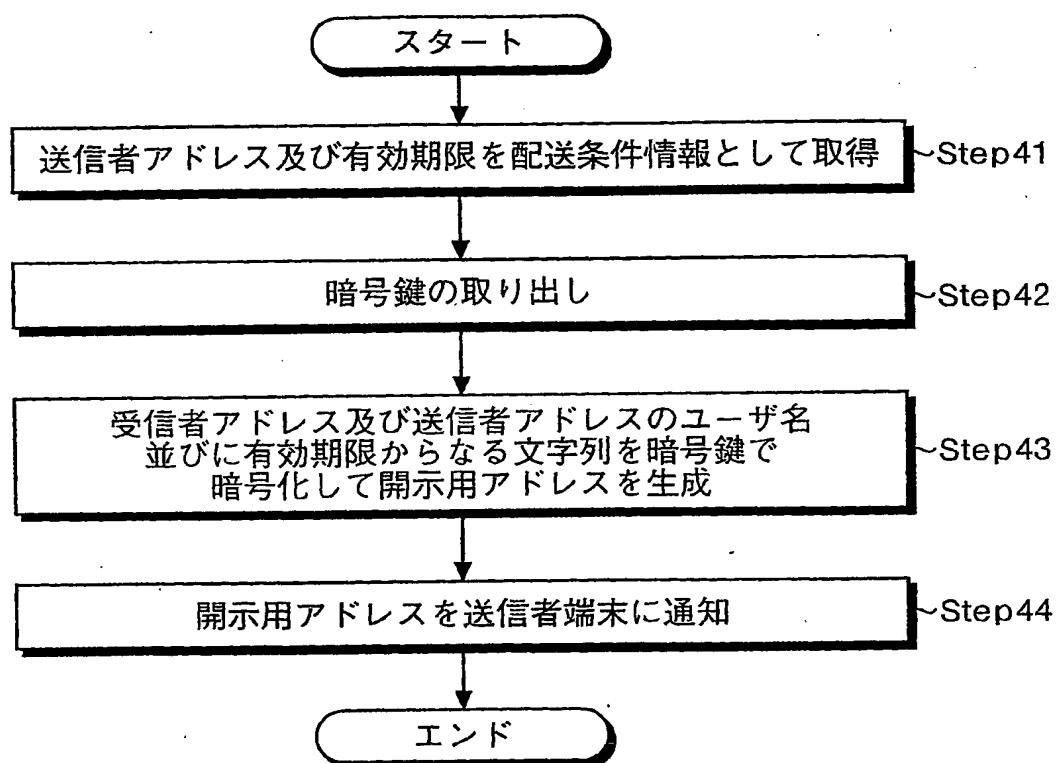
## 第2図



## 第3図



## 第4図

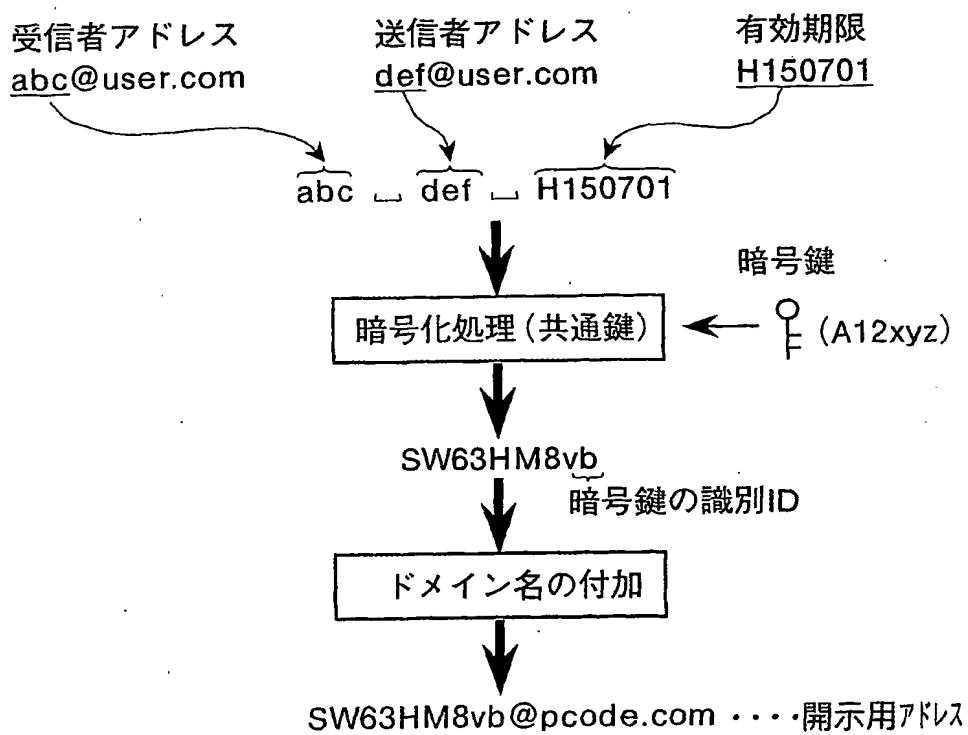


## 第5図

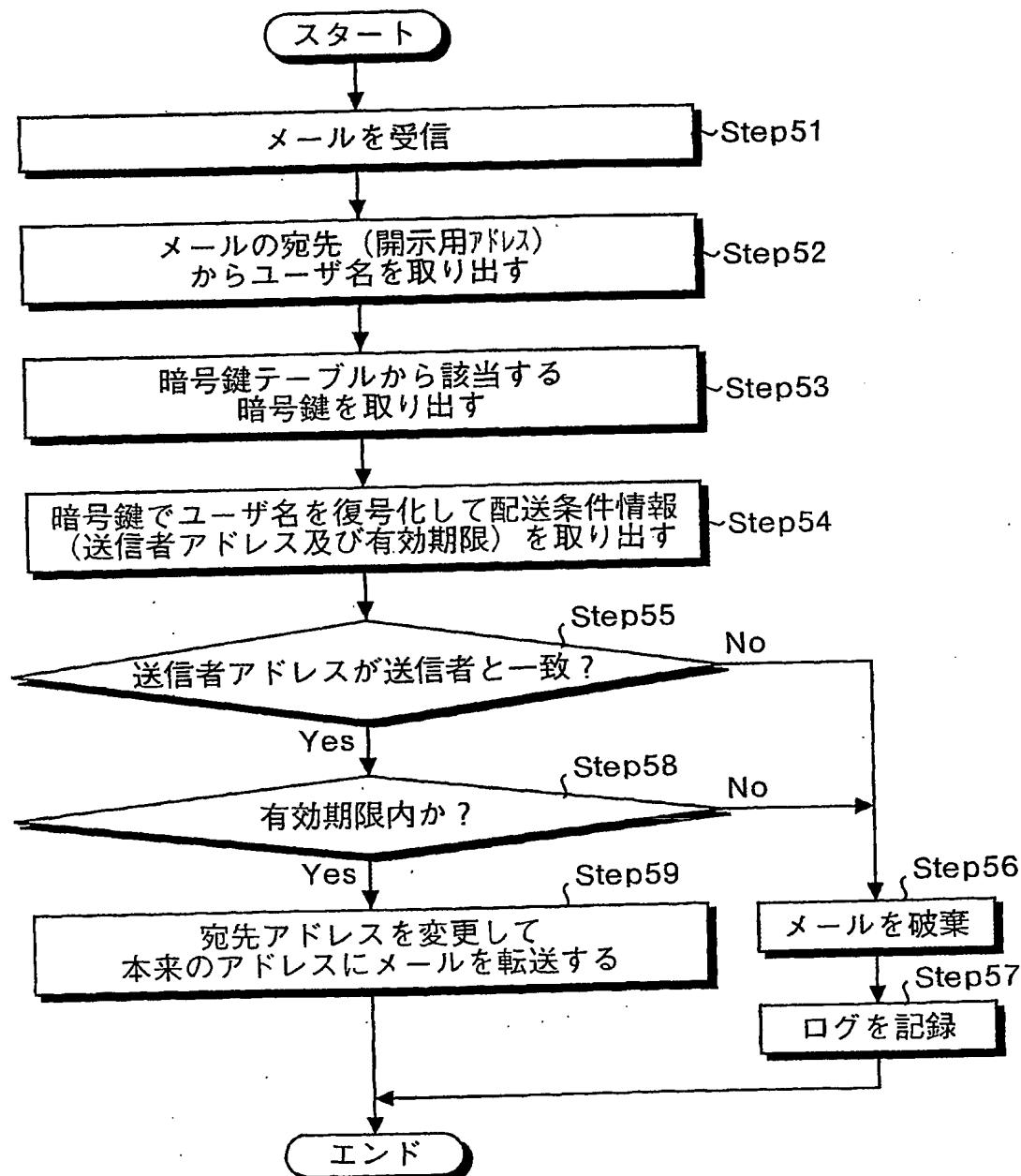
120

開示用アドレス生成ページ	
受信者アドレス：	abc@user.com ~121
送信者アドレス：	def@user.com ~122
有効期限：	H15.07.01 ~123
124	
OK	CANCEL
開示用アドレス： SW63HM8vb@pcode.com ~125	

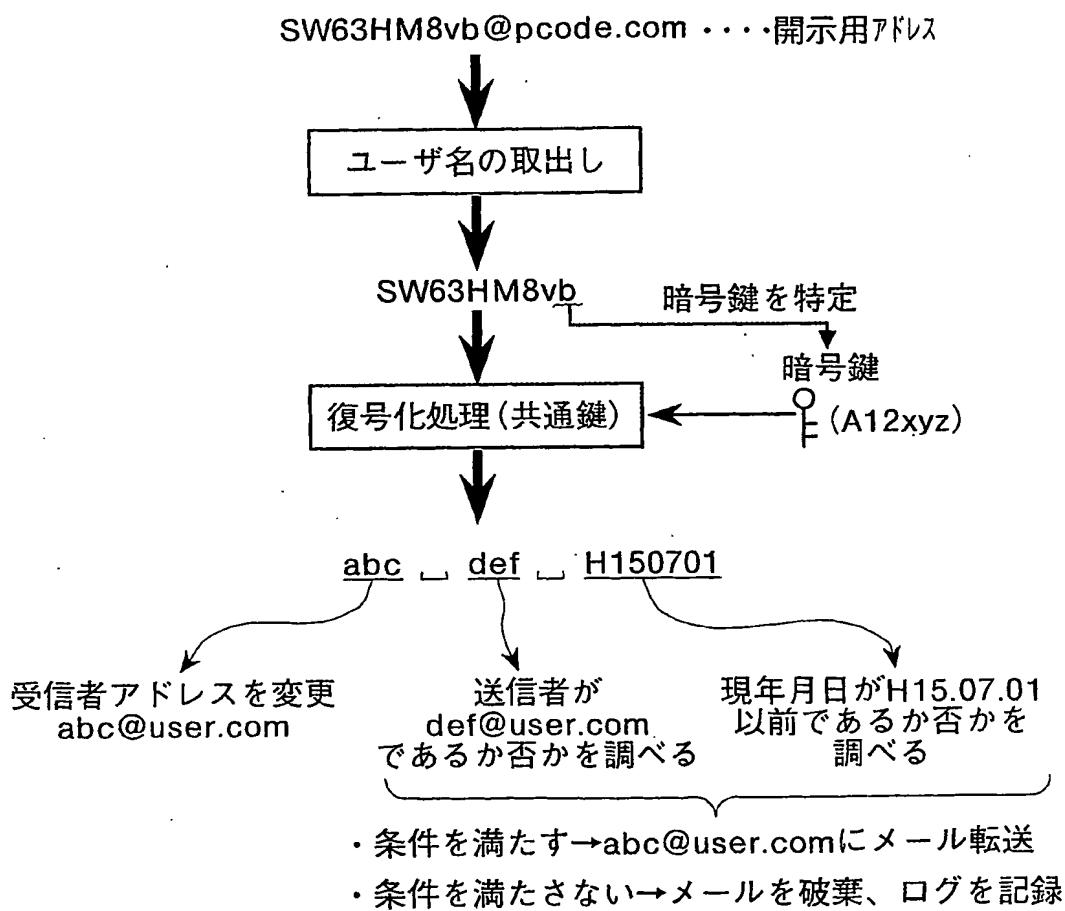
## 第6図



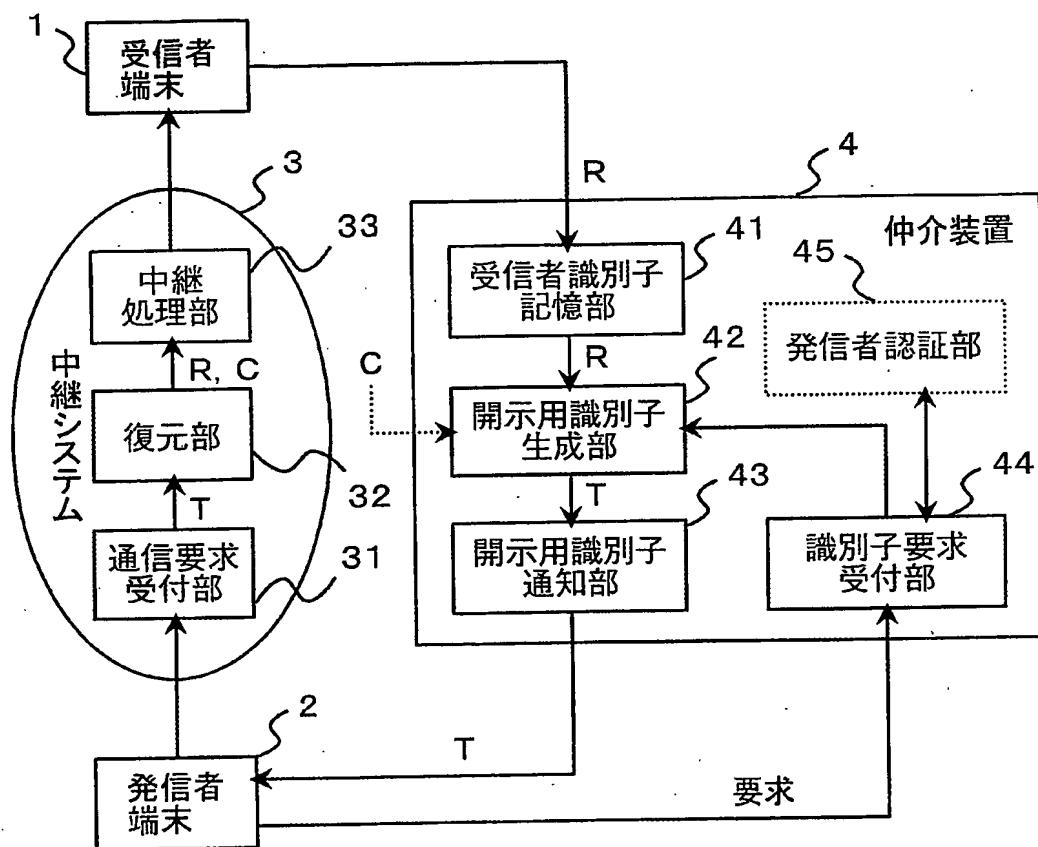
## 第7図



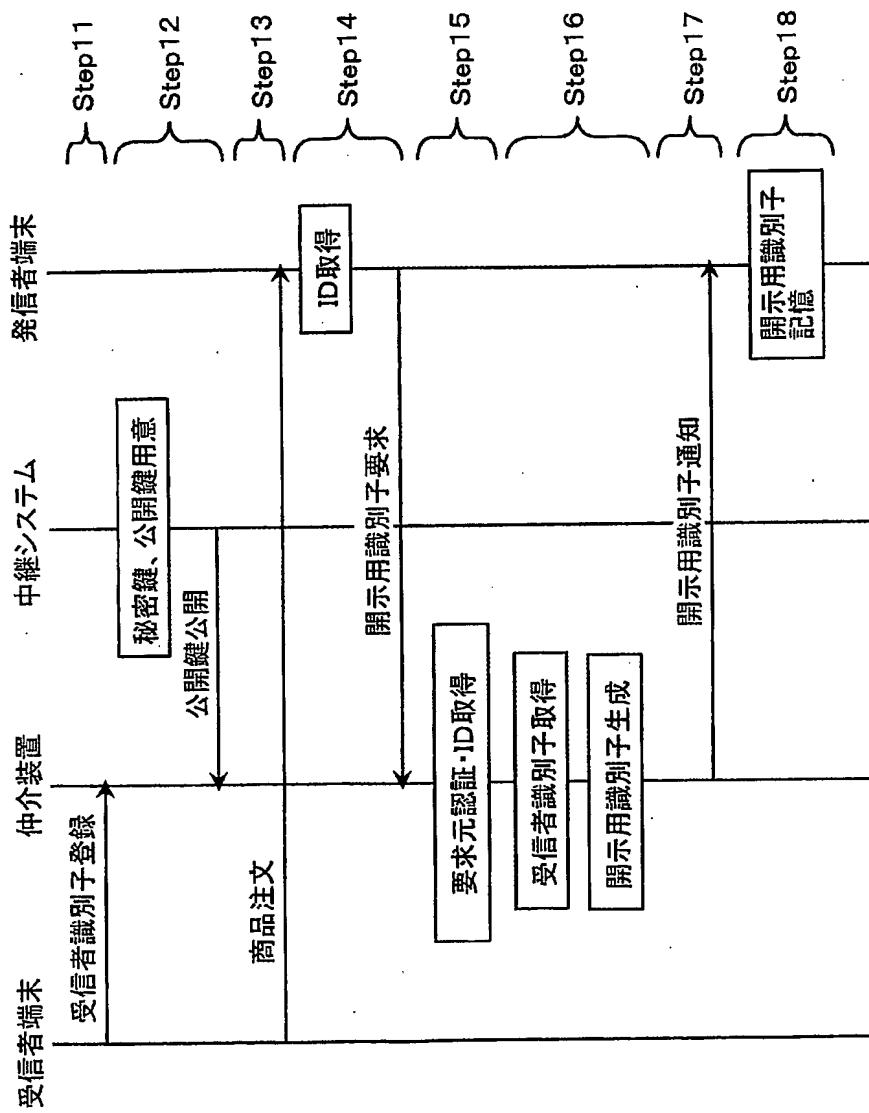
## 第8図

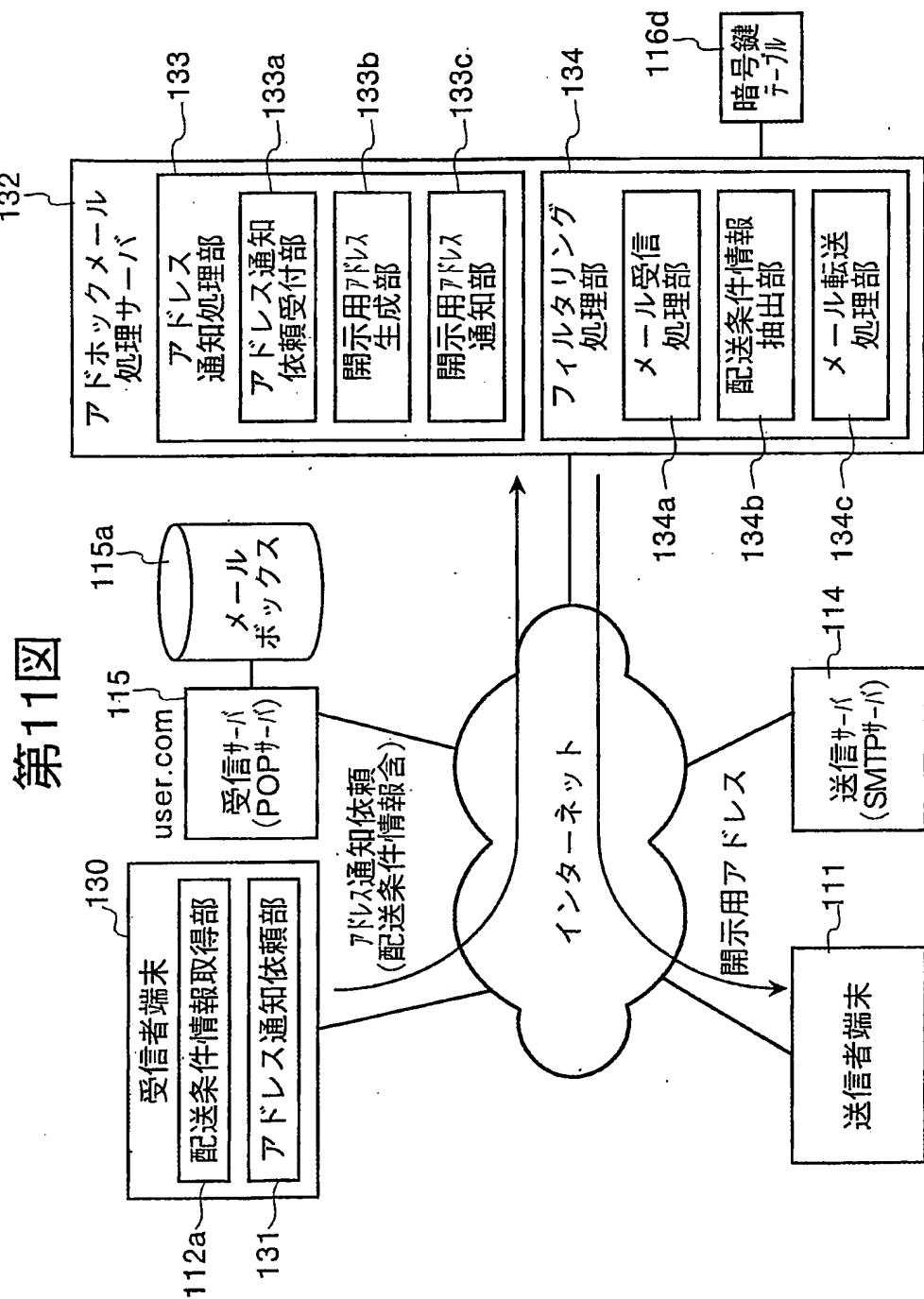


第9図

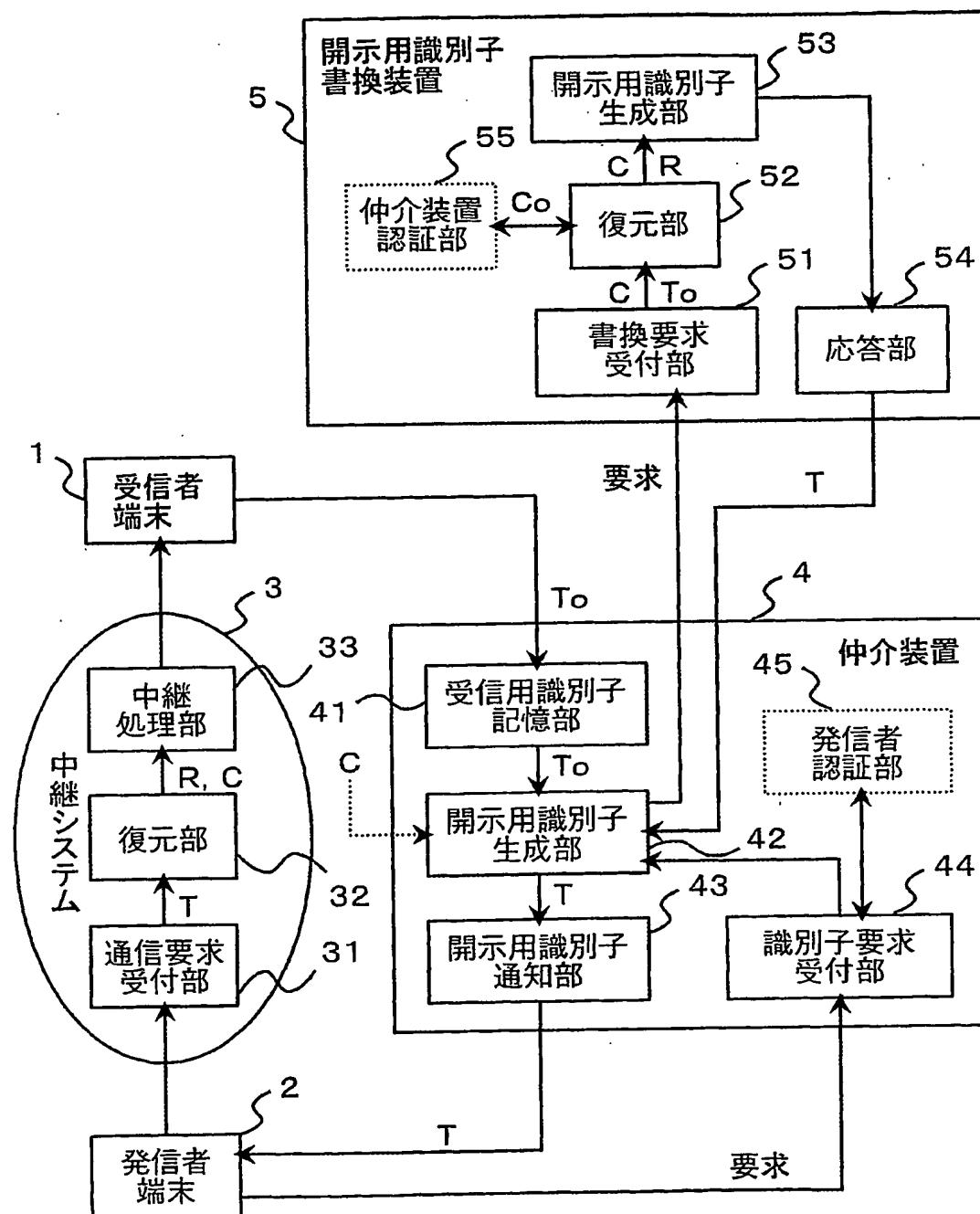


第10図

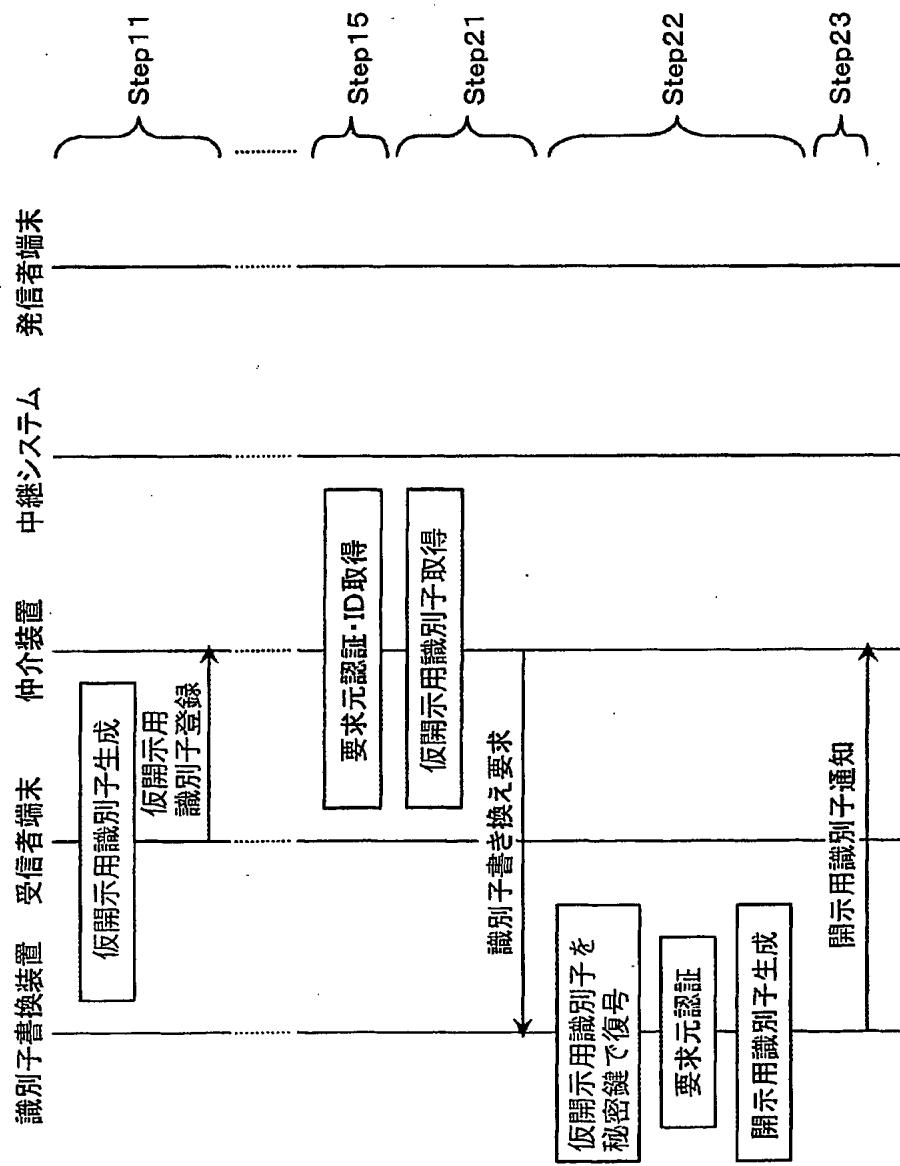




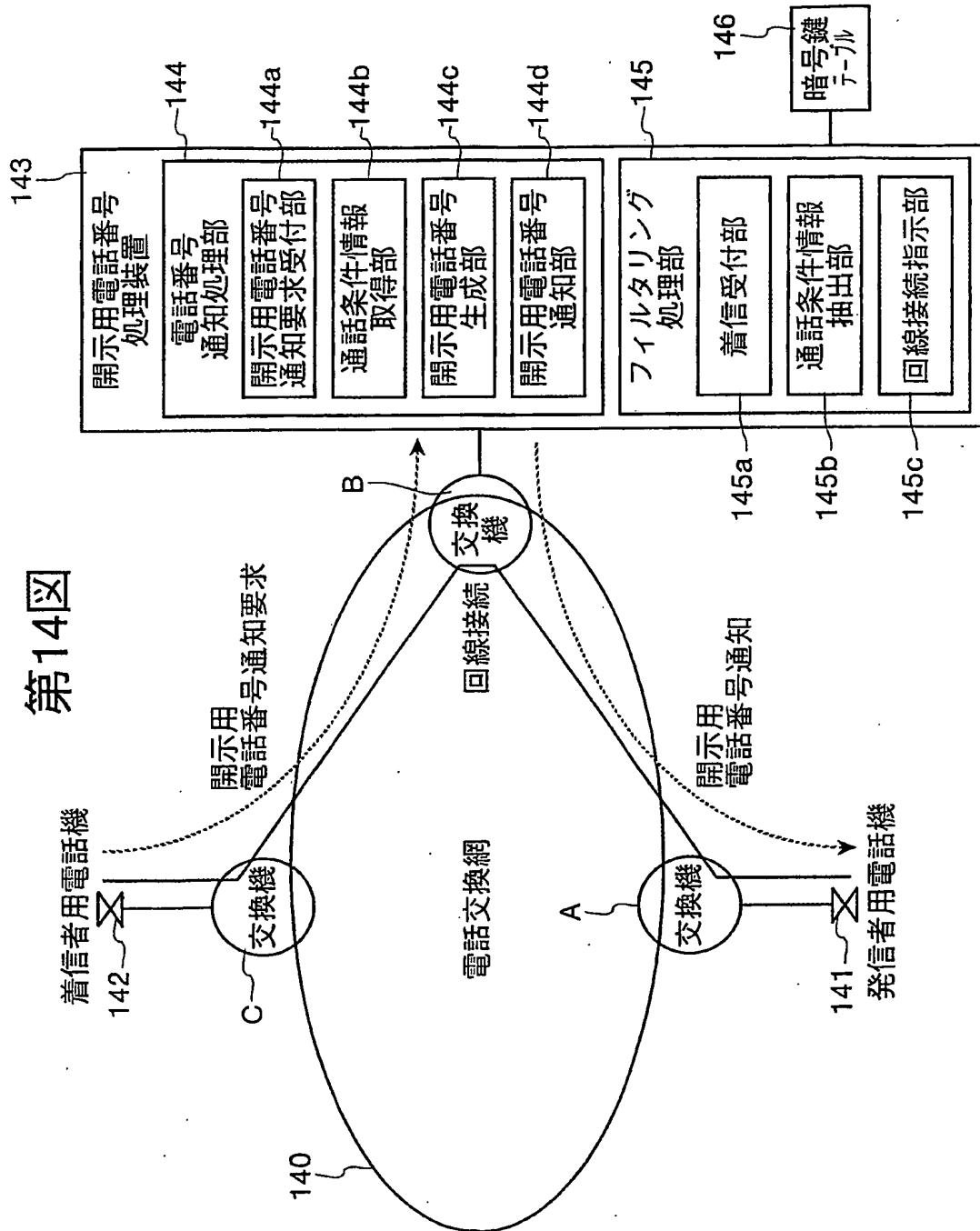
## 第12回



## 第13回

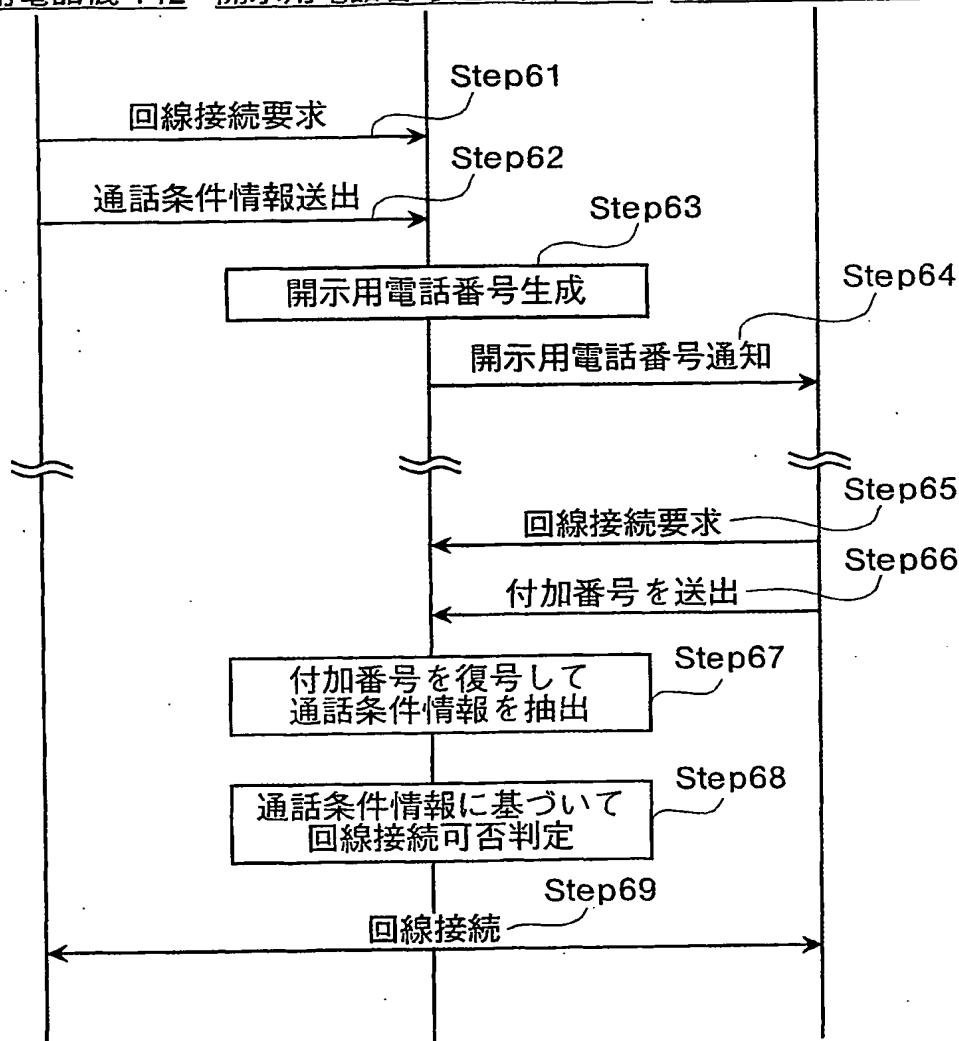


第14回

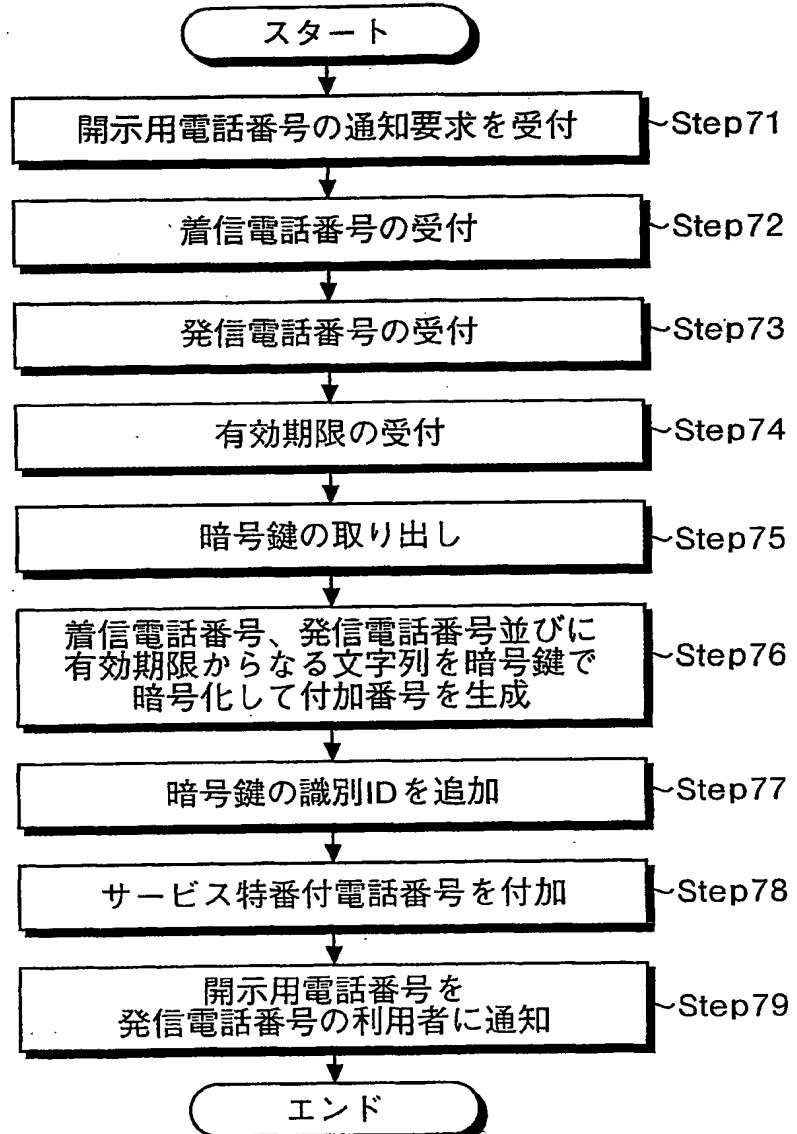


## 第15図

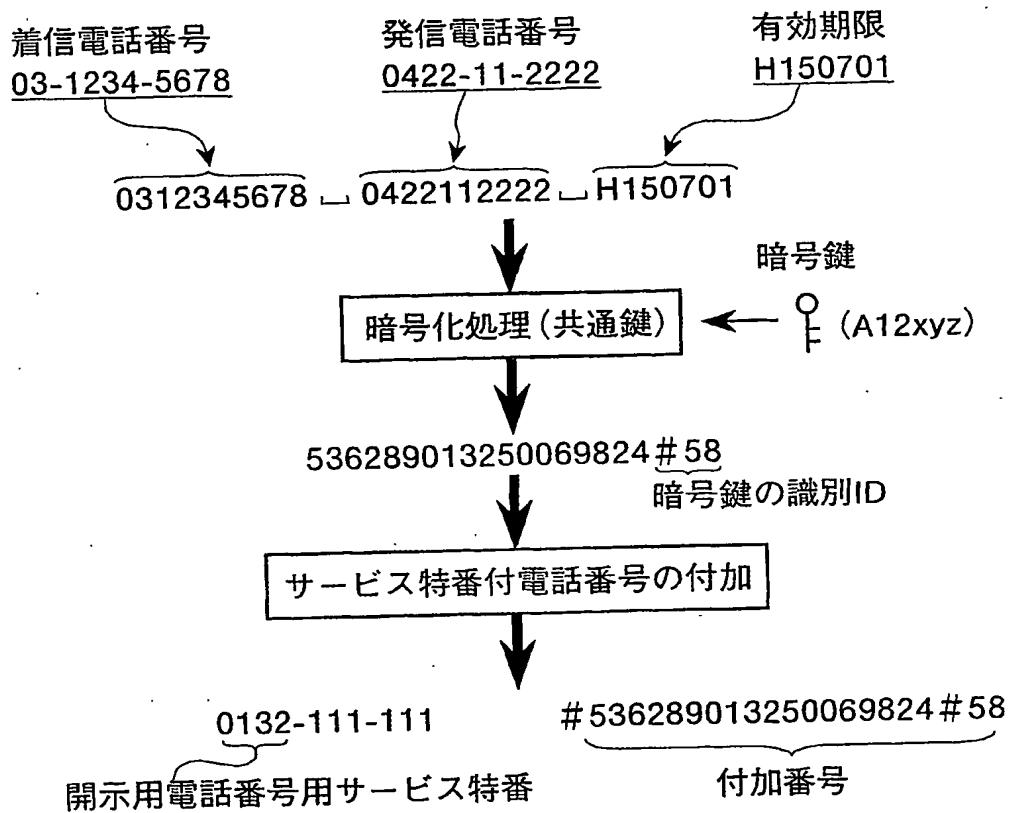
着信者用電話機 142 開示用電話番号処理装置 143 発信者用電話機 141



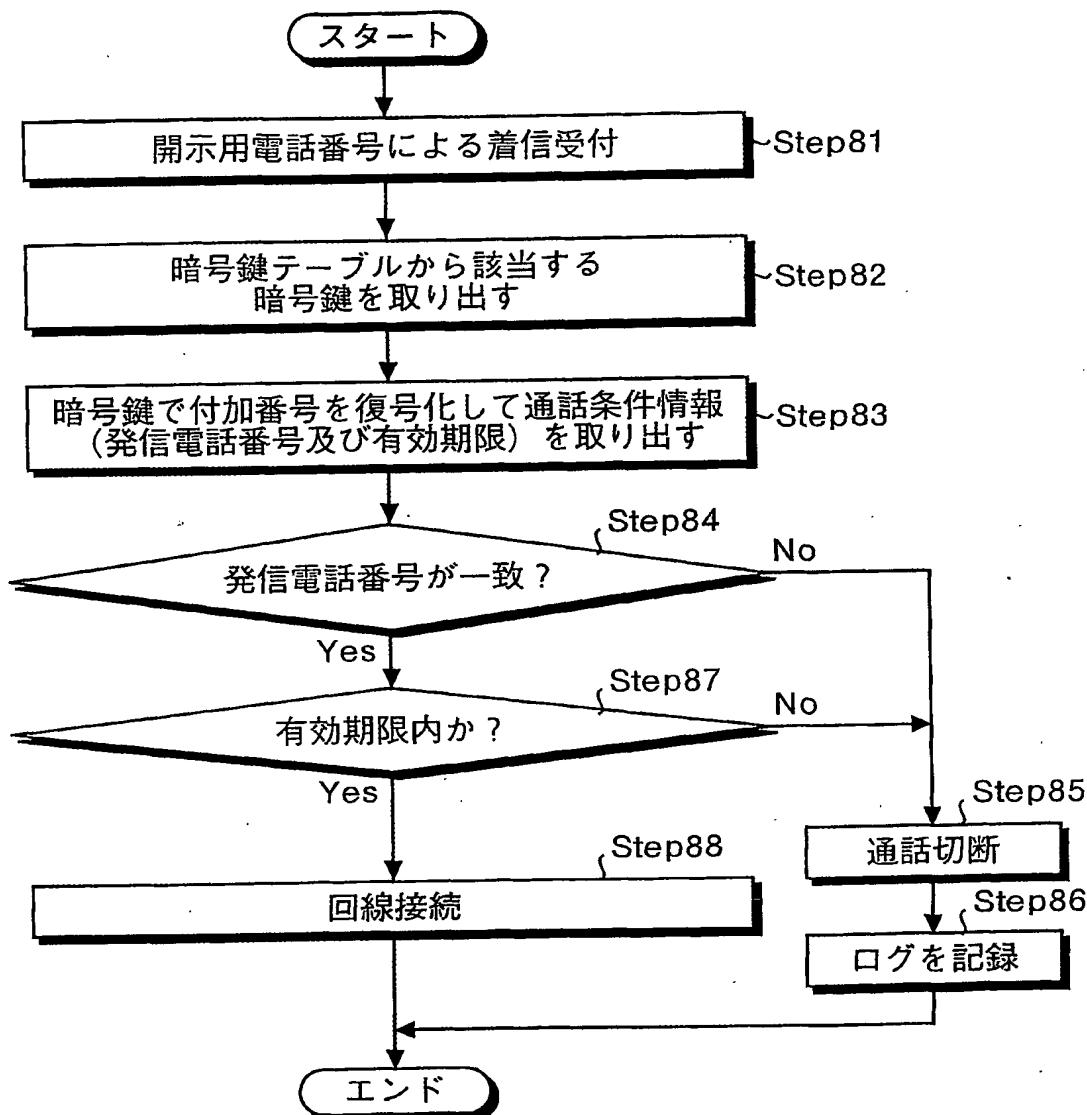
## 第16図



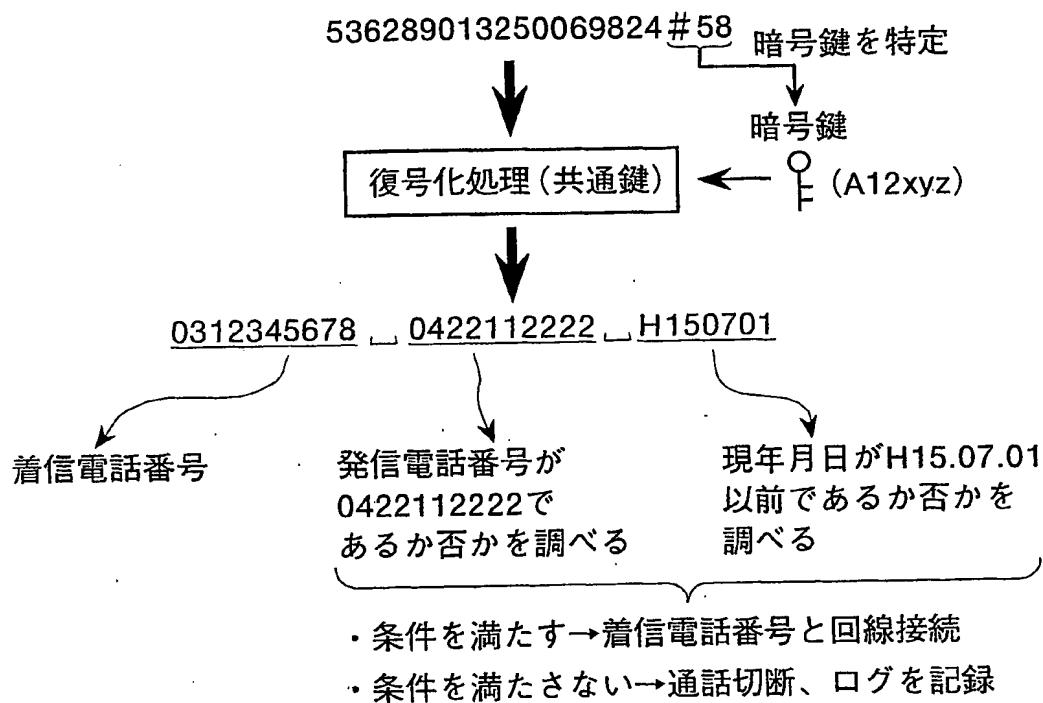
## 第17図



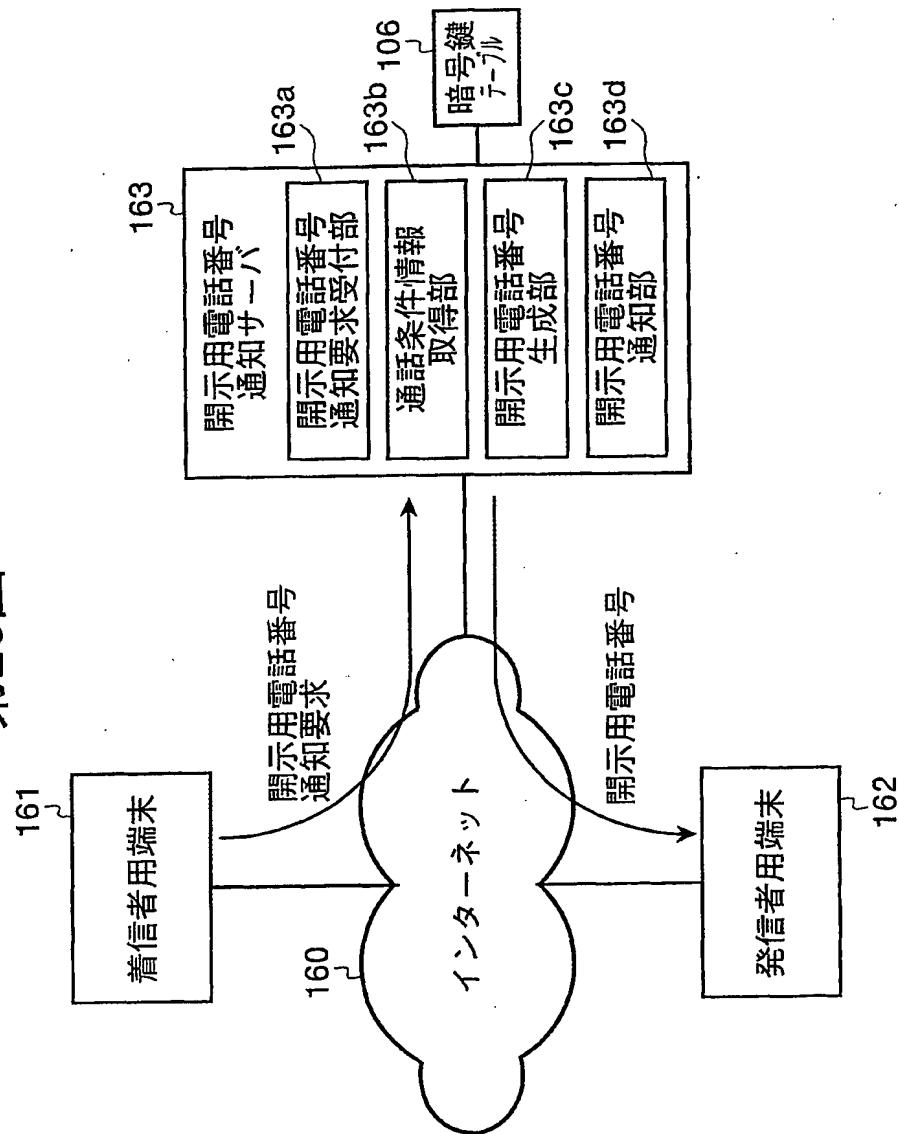
## 第18図



## 第19図



第20図



21/41

## 第21図

170

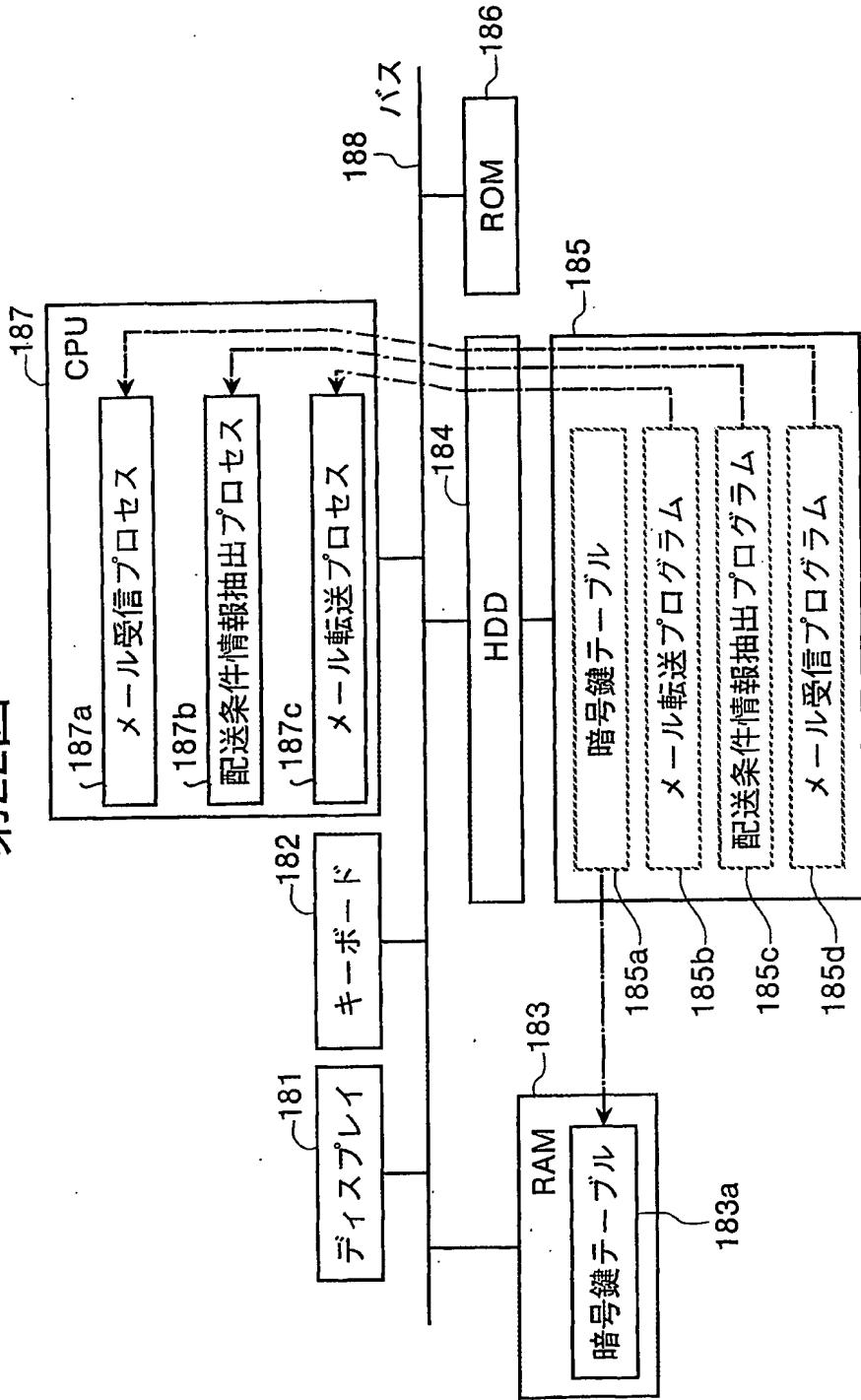
開示用アドレス生成ページ		
着信電話番号 :	03-1234-5678	171
発信電話番号 :	0422-11-2222	172
有効期限 :	H15.07.01	173
174		
OK	CANSEL	

175

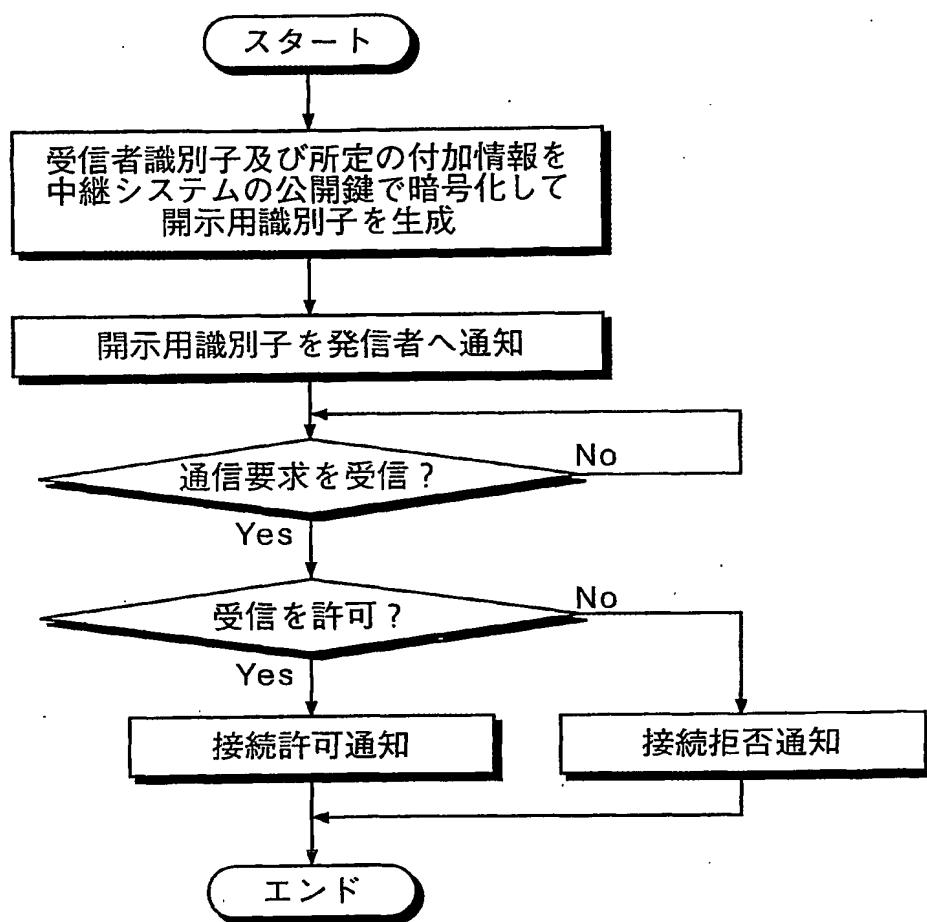
開示用電話番号

0132-111-111 # 536289013250069824 # 58

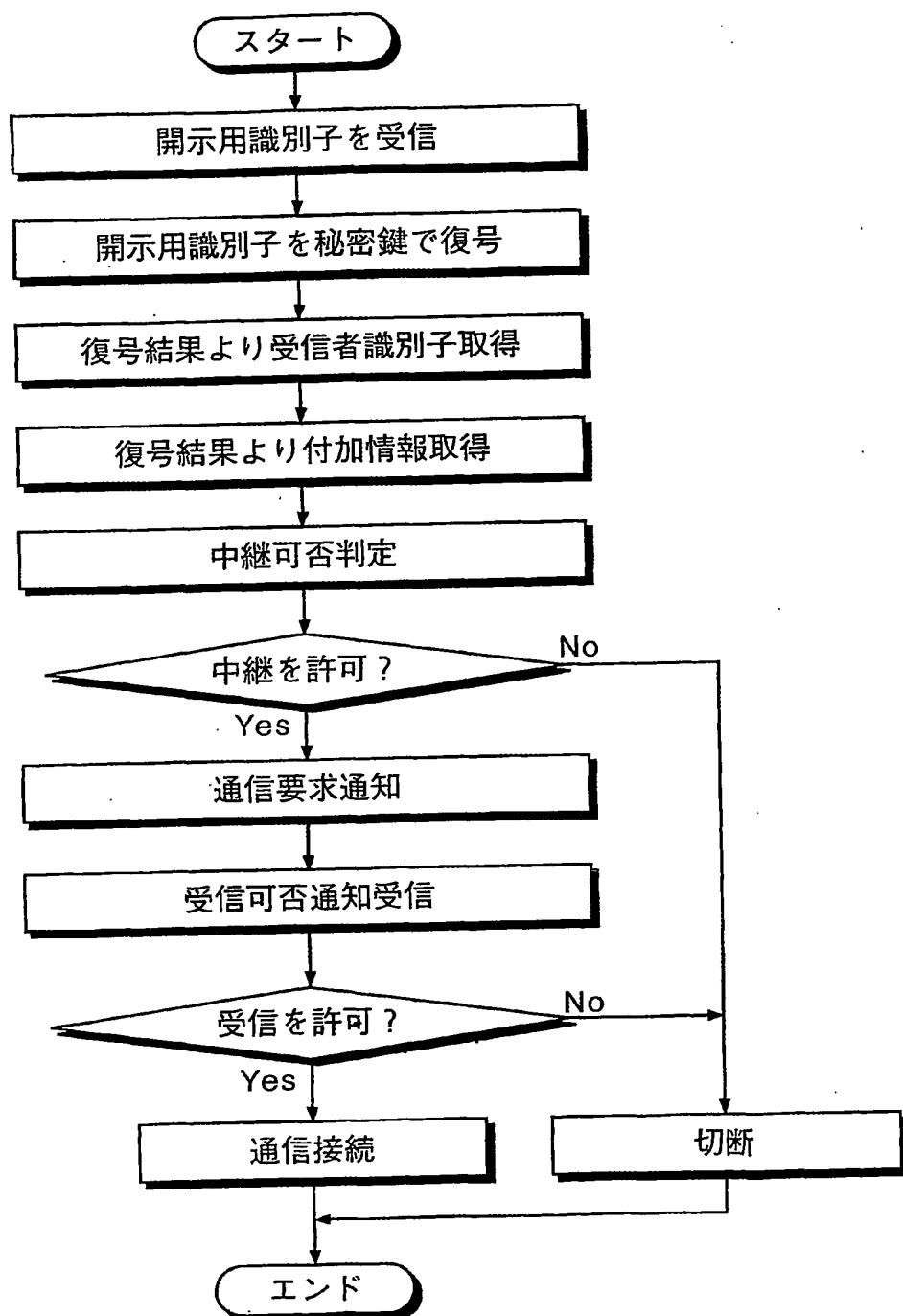
## 第22図



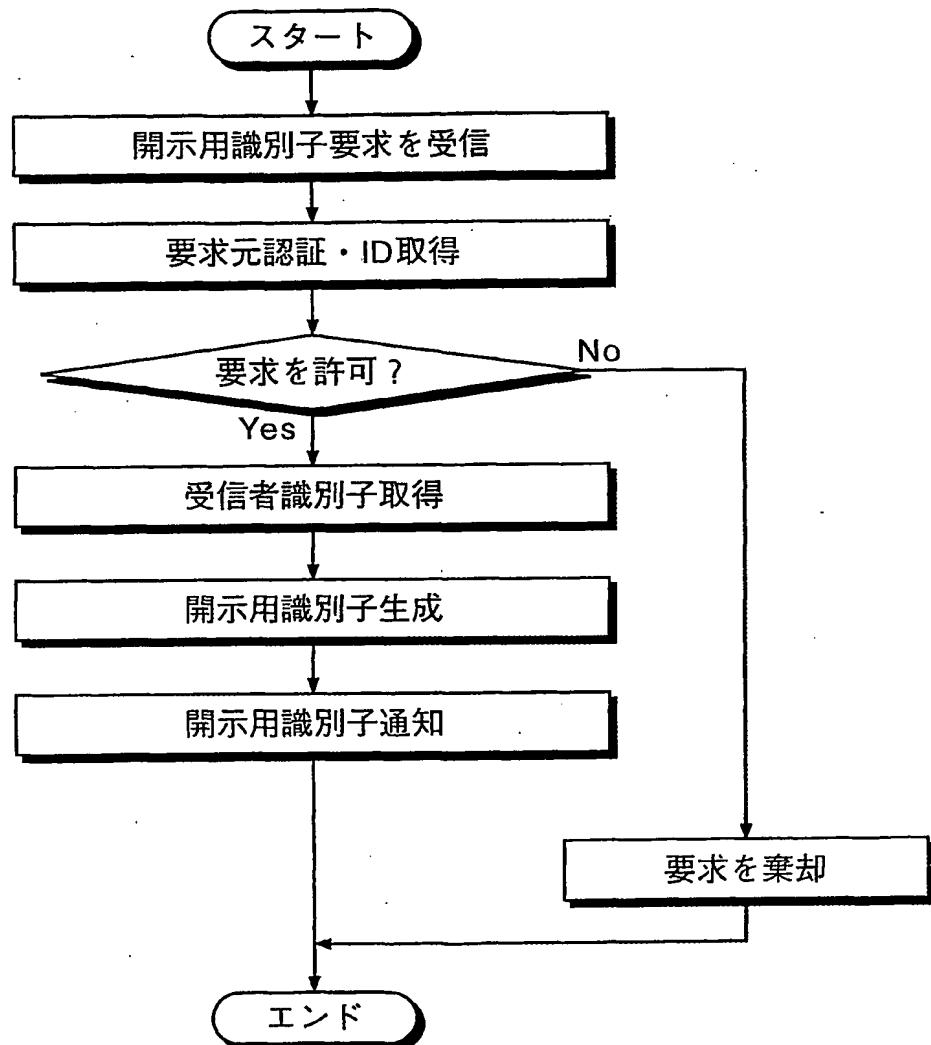
## 第23図



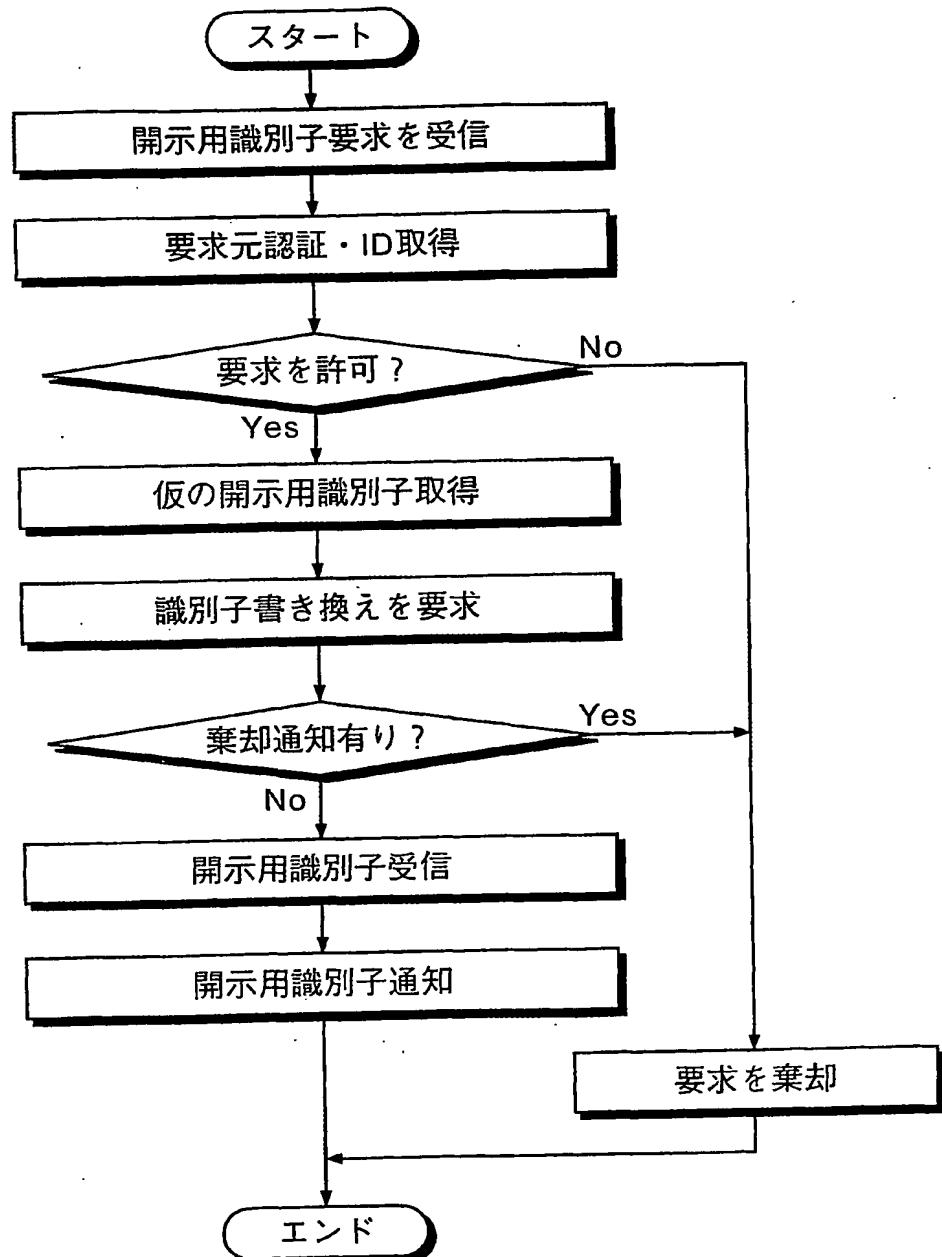
## 第24図



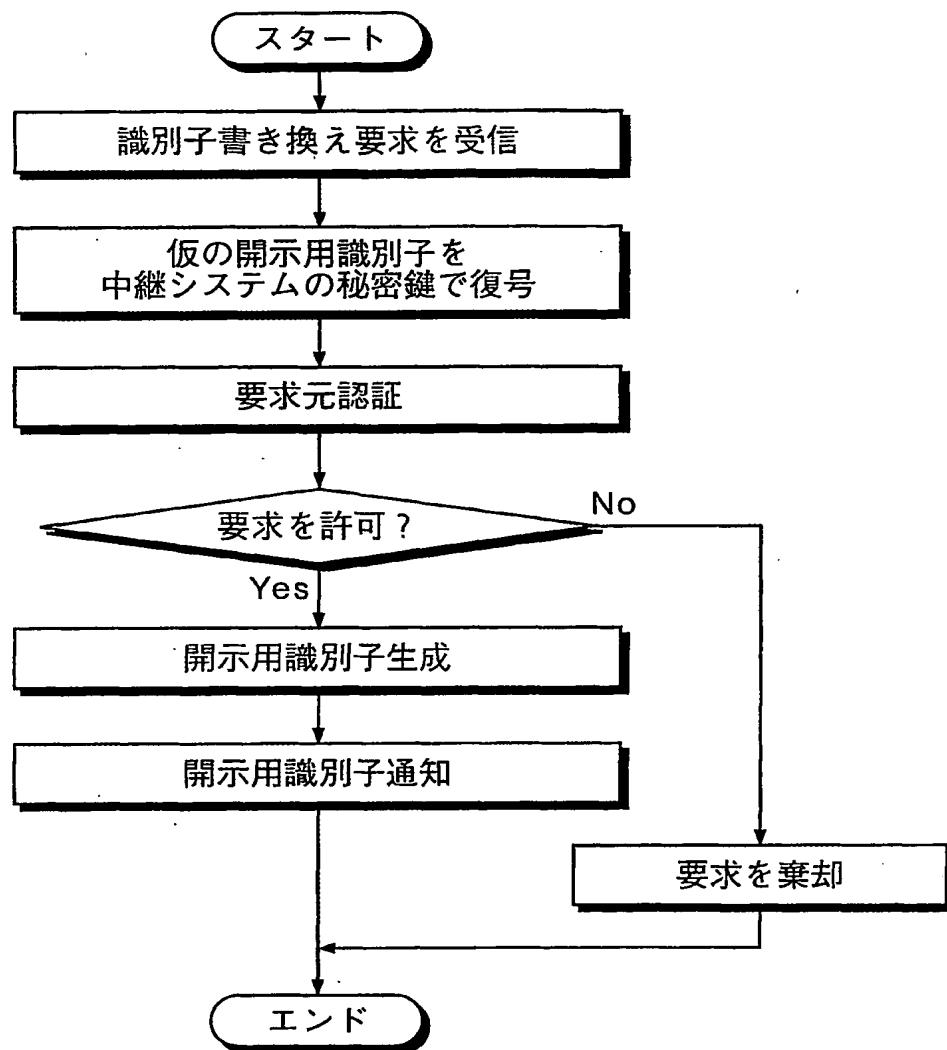
## 第25図



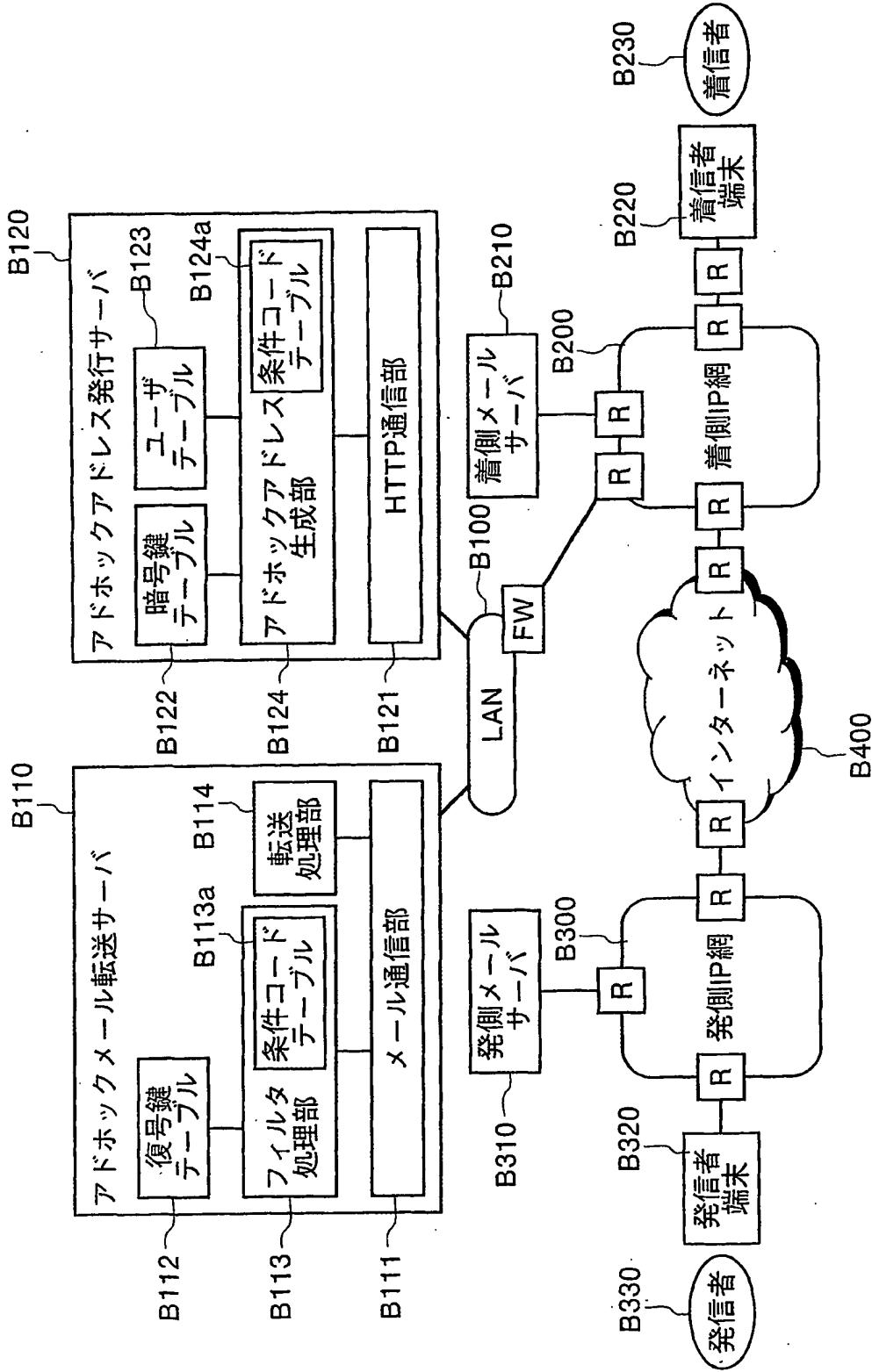
## 第26図



## 第27図



第28図



## 第29図

B112 暗号鍵テーブル

鍵ID(ID_K)	鍵(K)
17	0x34d2a36b
18	0xe48ab21f
19	0xab46fc9a
20	0xe6a3b13b
...	

## 第30図

B123 ユーザテーブル

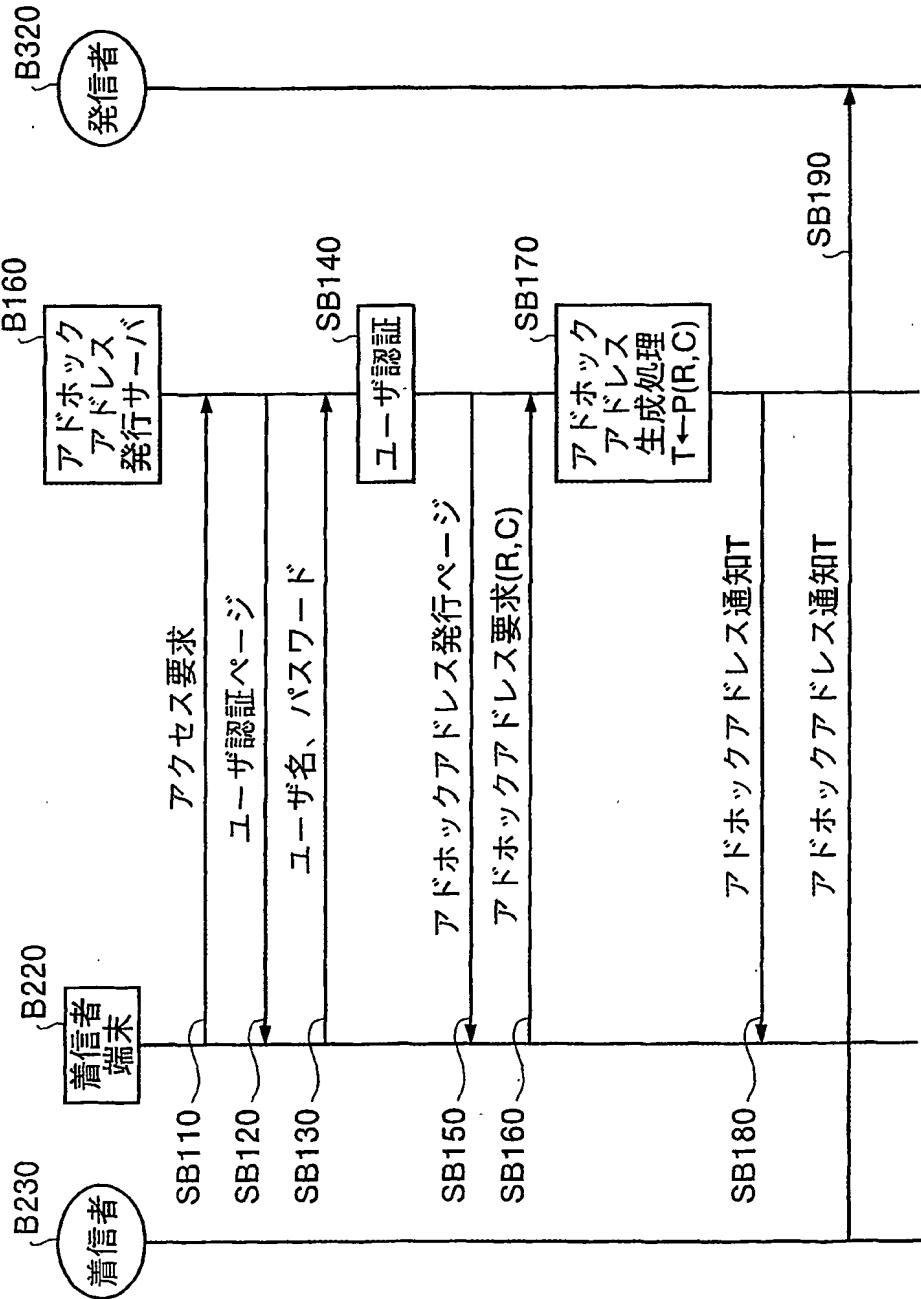
ユーザ名	パスワード
...	
suzuki	ef34szq5s
tanaka	ew4902sa
...	
yamada	wf4wsfa3s

## 第31図

B124a 条件コードテーブル

組み合わせ パターン	組み合わせ コード
S	0000
D	0001
E	0010
F	0011
SE	0100
DE	0101
DF	0110
DEF	0111

## 第32回



32/41

## 第33図

B500

ユーザ認証ページ

ユーザ名	tanaka
パスワード	*****
送信	キャンセル

## 第34図

B600

アドホックアドレス発行ページ

ユーザ名 tanaka

着信者アドレス tanaka@mail.isp-A.ne.jp

配送条件

発信者指定 なし  あり(アドレス指定)  あり(ドメイン指定)

ありの場合の指定アドレスまたはドメイン名 suzuki@mail.isp-B.ne.jp

有効期限 なし  あり

ありの場合の有効期限 2003 年 8 月 31 日

着信開始日指定 なし  あり

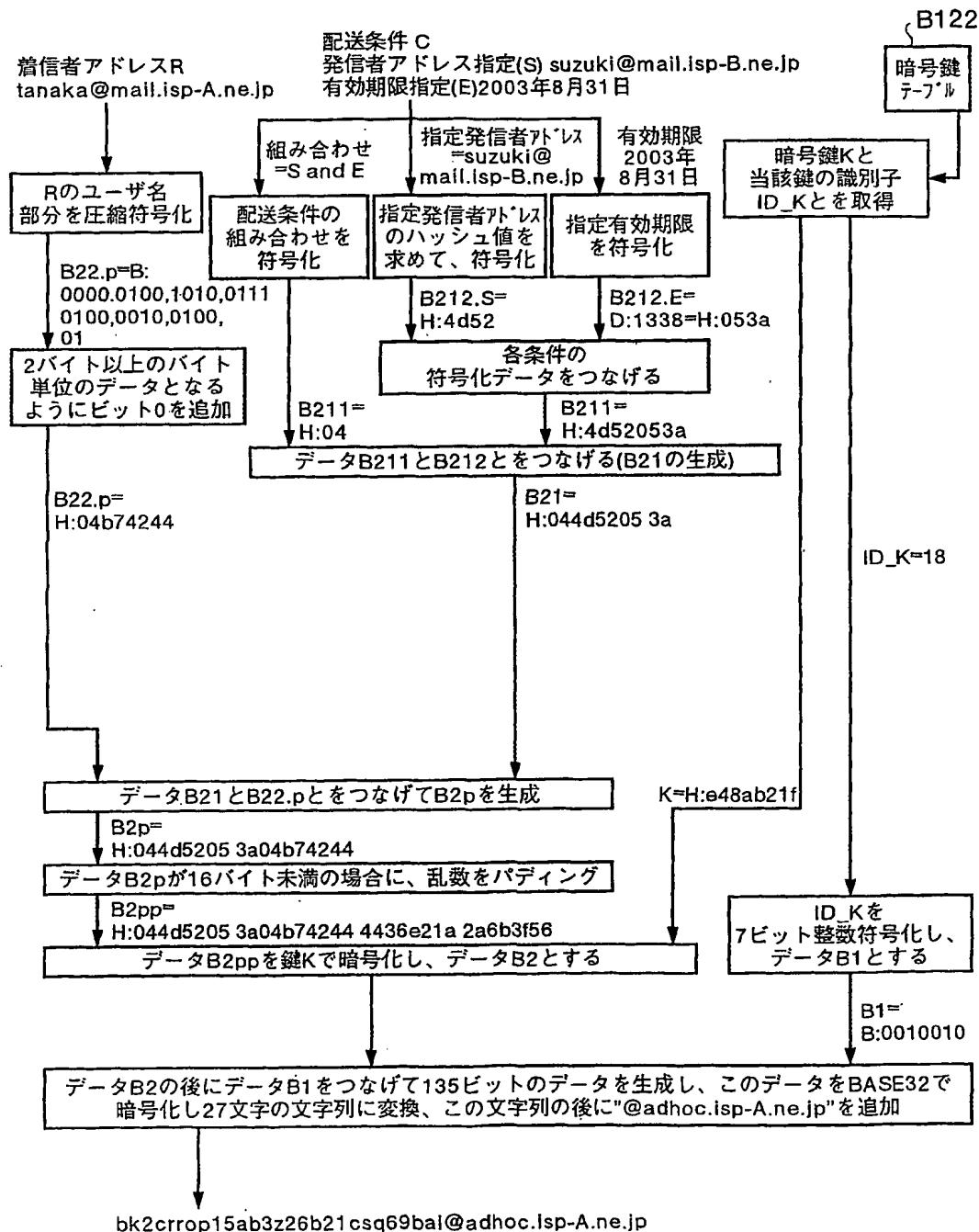
ありの場合の着信開始日 [ ] 年 [ ] 月 [ ] 日

送信 キャンセル

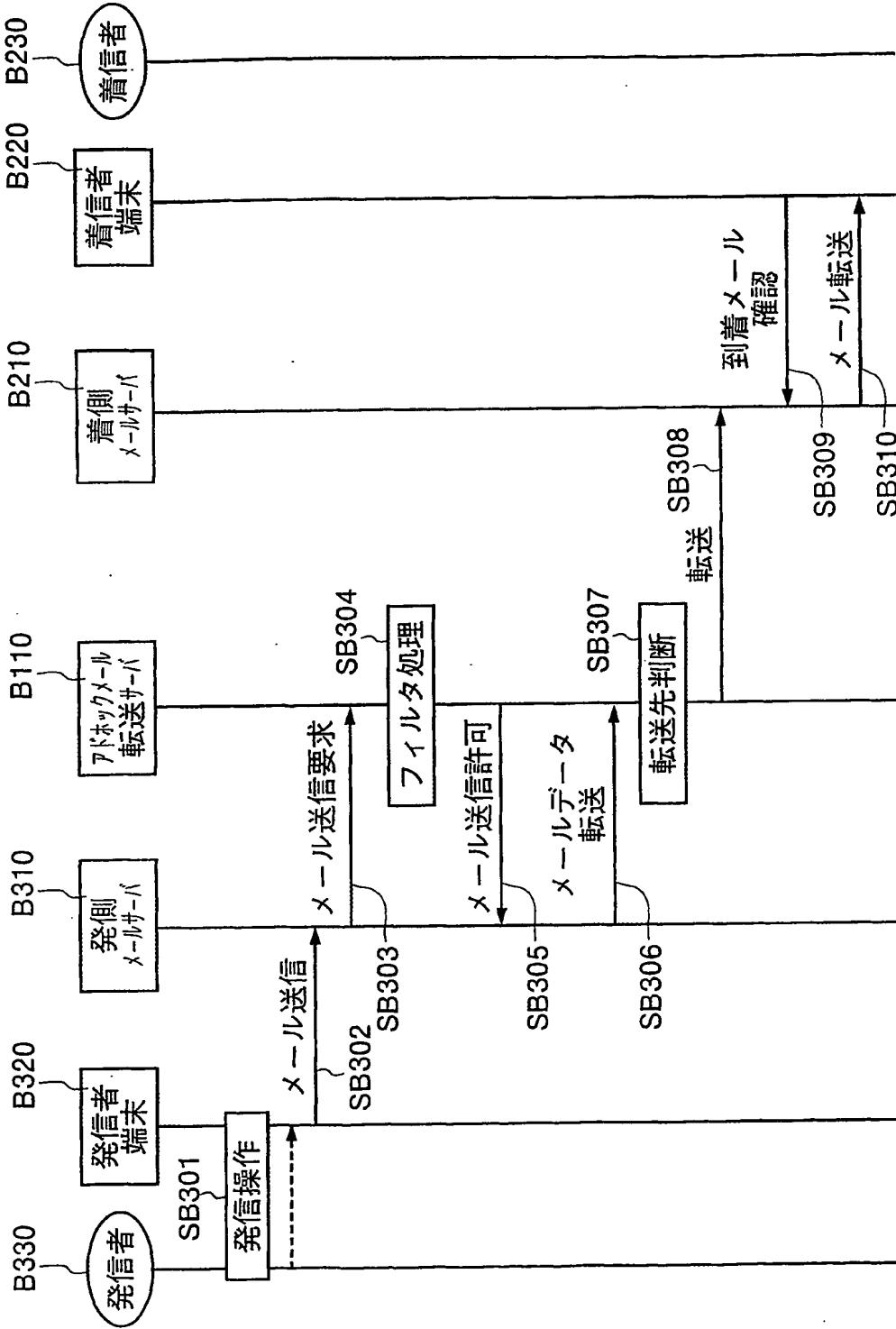
## 第35図



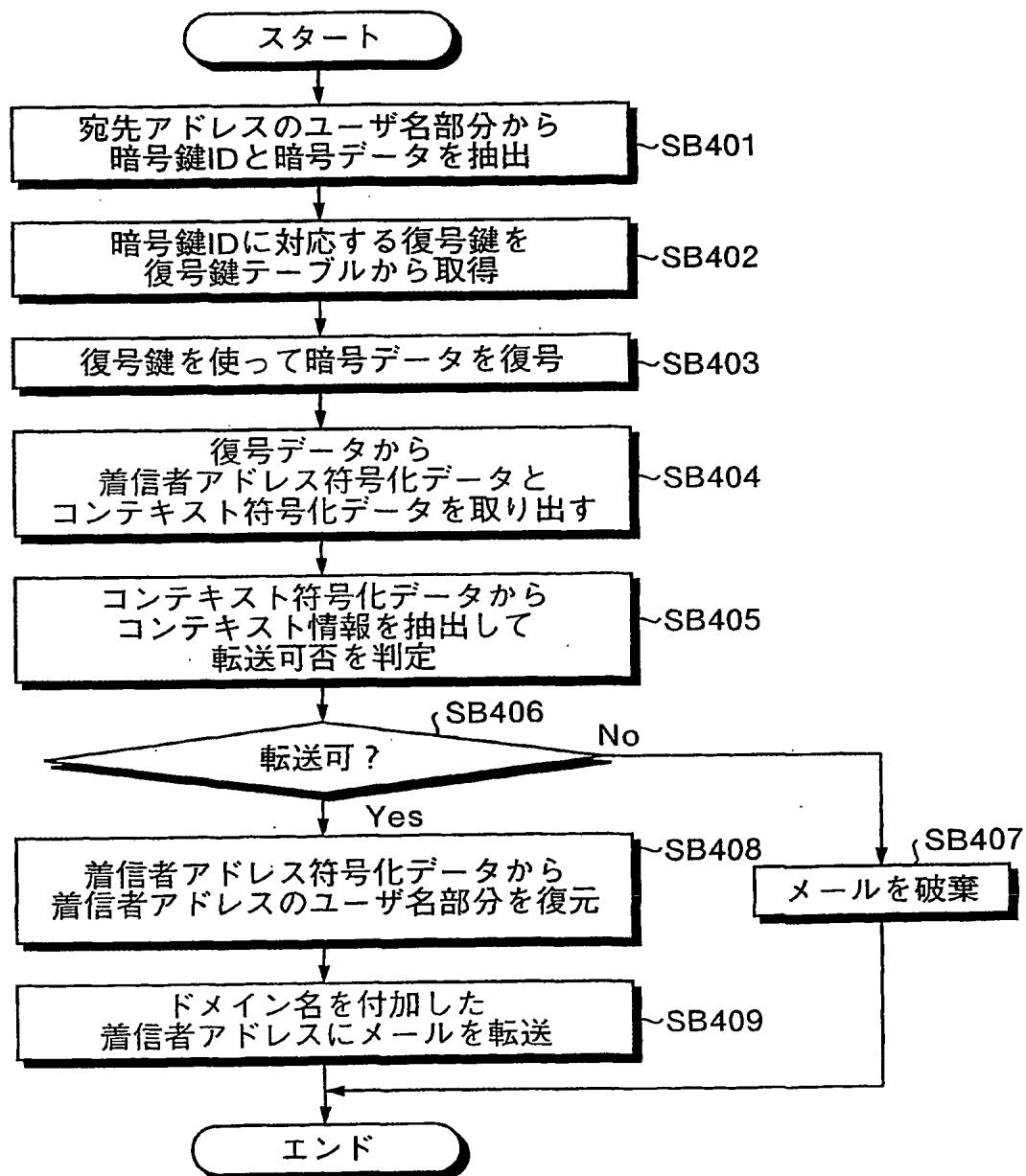
## 第36図



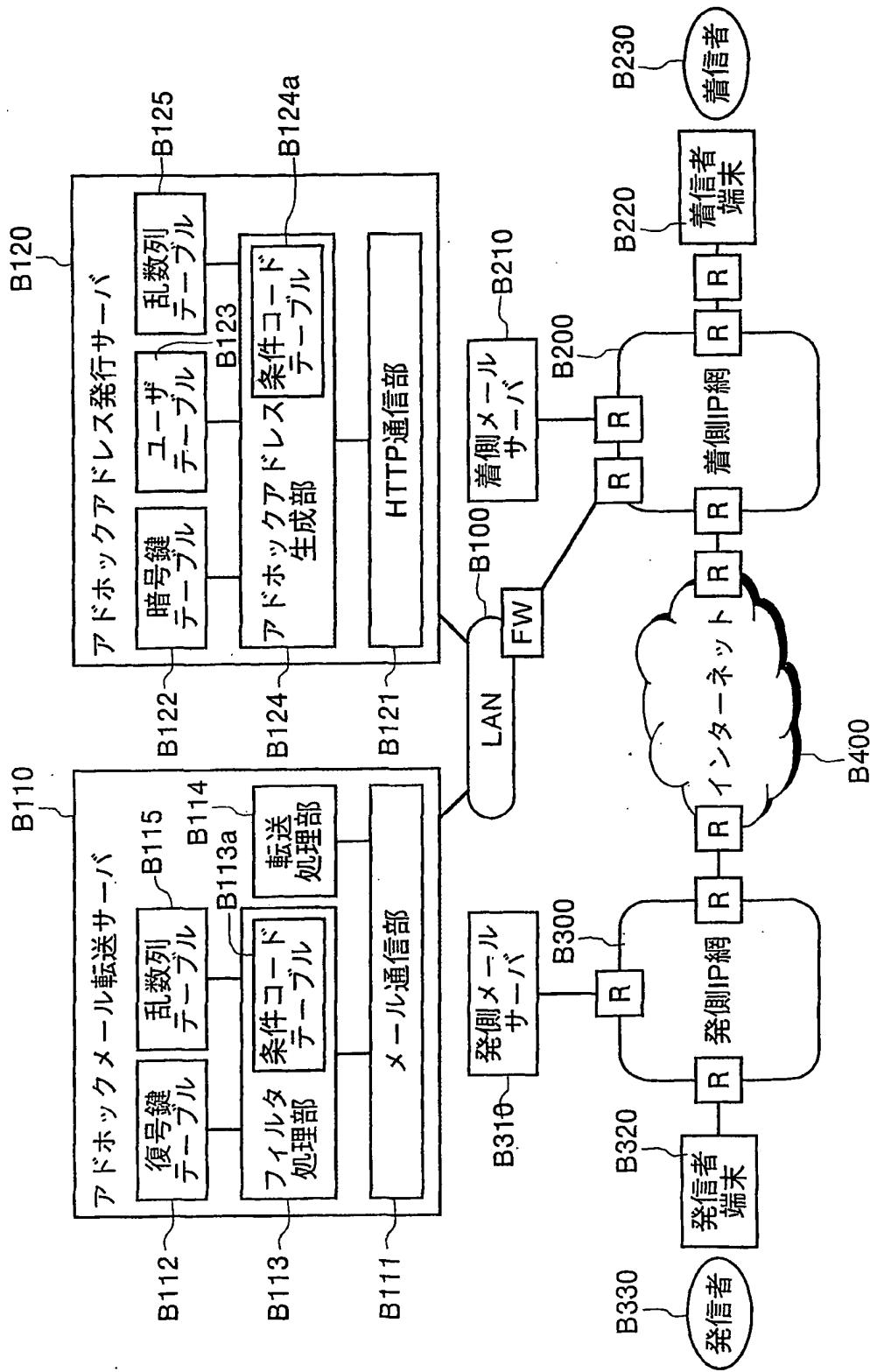
第37図



## 第38図



第39図

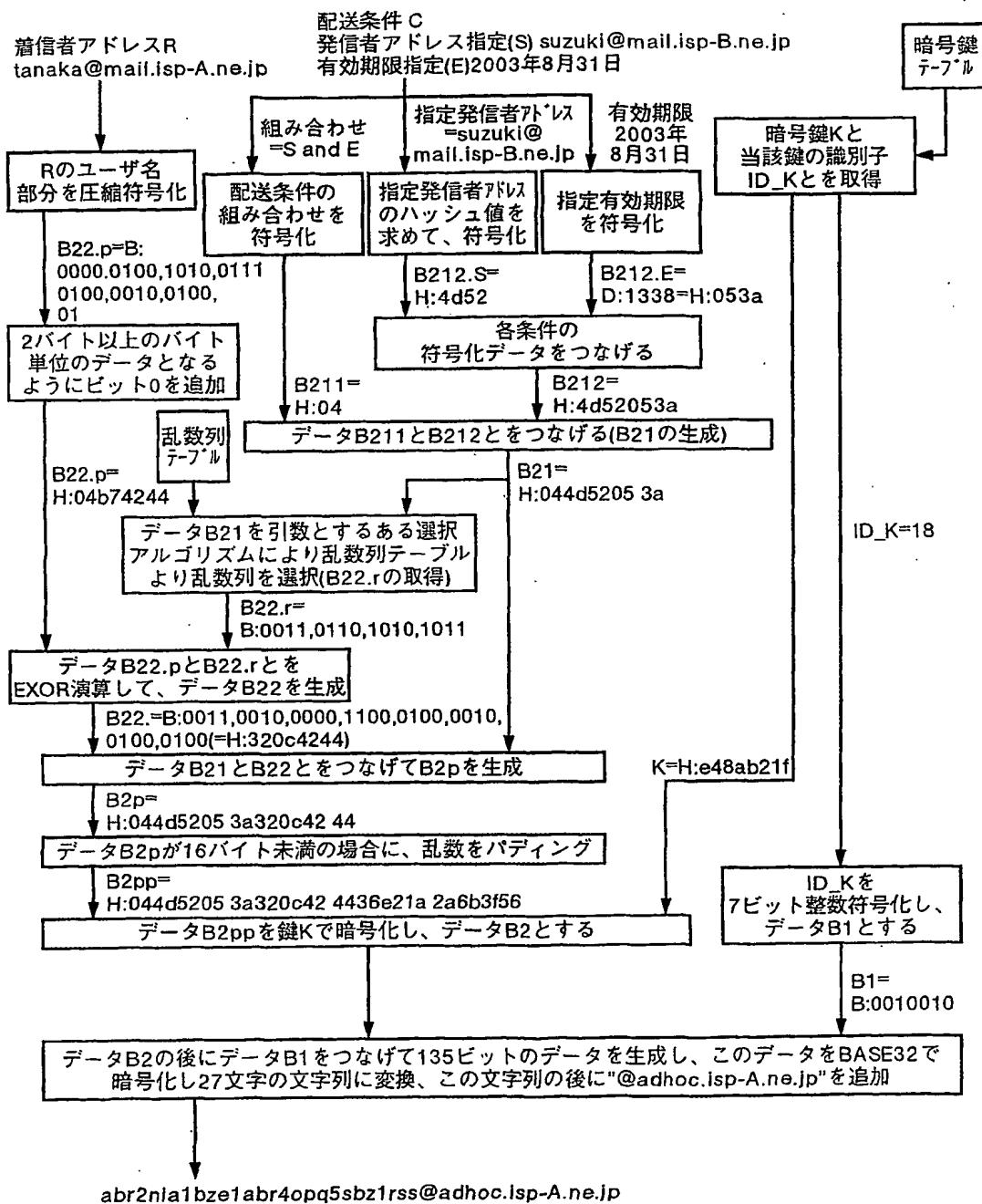


## 第40図

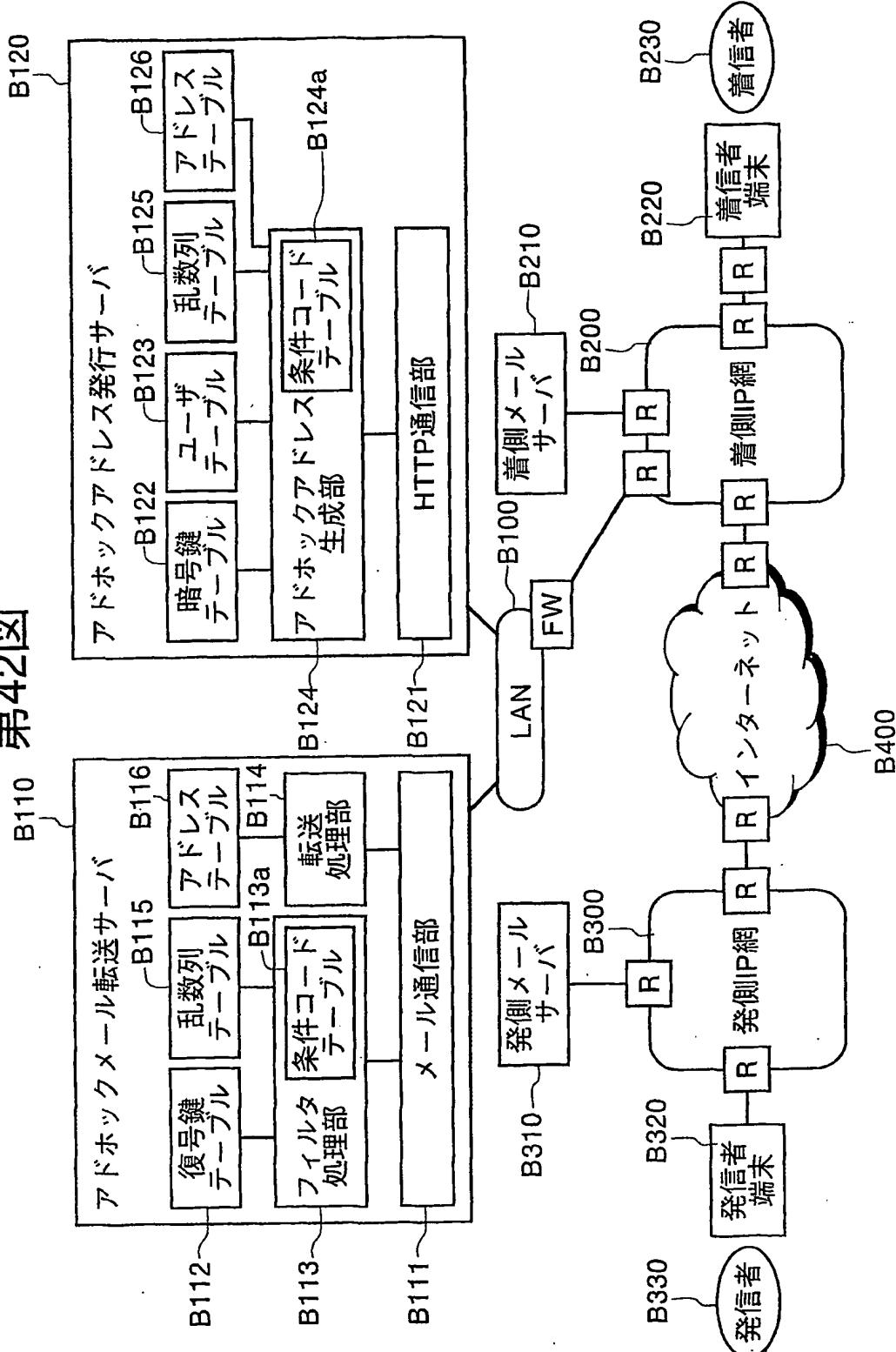
B125 亂数列テーブル

インデックス	乱数列
0	0101,0100,1010,1110
1	0111,0101,0100,0101
2	0011,0110,1010,1011
...	

## 第41図



第42回



## 第43図

B126 アドレステーブル

アドホックメールユーザID	着信者アドレス(R)
...	...
TN	tanap@oce.com
SZ	suzup@pla.com
...	...